

This project has received funding from the European Union's Horizon Innovation Actions - Sustainable, secure and competitive energy supply CL-5-2021-D3-01 under Grant Agreement: 101069839



Shaping consumer-inclusive data pathwaYs towards the eNERGy transition, through a reference Energy data Space implementation

WP1: Project Management

D1.1: Project Management Plan

Deliverable Leader: TXT Due Date: M3 Dissemination Level: PU – Public Version: 1.0

Disclaimer. The views represented in this document only reflect the views of the authors and not the views of the European Union. The European Union is not liable for any use that may be made of the information contained in this document. Furthermore, the information is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user of the information uses it at its sole risk and liability.



Document Log

Contributors	Francesca Lazzari (TXT), Veronica Antonello (TXT), Mirco Mariani (TXT), Michele Sesana (TXT), Dimitra Stefanatou (ALBV), Fa Somers (ALBV), Toygar Hasan Oruc (ALBV), Fenareti Lampathaki (Suite5)
Internal Reviewer 1	ICCS
Internal Reviewer 2	HEDNO
Туре	R — Document, report

History

Versions	Date	Description
0.1	07/10/2022	TOC definition
0.2	18/11/2022	First contribution on chapters 1,2,3,4,6,7
0.3	24/11/2022	Updates chapters 1,2,3,4 and new contribution on chapter 5
0.4	25/11/2022	First consolidated version for peer-reviewers
0.5	28/11/2022	Revision of internal reviewers
1.0	30/11/2022	Final version for the EC



Executive Summary

The "Project Management Plan" describes the processes and tools that are applied in the SYNERGIES project to ensure high-quality of the SYNERGIES deliverables and of the overall project management activities. The present document identifies the structure, processes, timeline and tools that shape the project organisation and work.

SYNERGIES consists of 22 partners from 11 countries, namely Italy, Spain, Greece, Cyprus, Denmark, Ireland, The Netherlands, Finland, Romania and Belgium. The SYNERGIES Grant Agreement, the Consortium Agreement and the Contacts living documents define the roles (Project Coordinator, Technical Coordinator, WP leader, etc), responsibilities and contact points for all the project participants, as well as a complete list of all involved people (mail). A detailed Project management structure including specific entities and management operational bodies has been identified to ensure a solid implementation of the project activities.

Rules and processes have been defined to shape the interactions among the project partners and the alignment of the scientific and technical activities, including the correct involvement of the demo sites and end-users.

Assuring the quality of the documents produced is critical and it touches upon several project activities, in terms of technical, communication, dissemination and exploitation activities. In this regard, a quality assurance process has been defined, including standard procedures to create the project documents (Deliverables) and periodical reporting, and to tackle potential deviations (conflicts, changes to the activities). Moreover, a set of tools has been developed to ensure optimal internal communication and coordination and uniformity of SYNERGIES documents and messages both in terms of graphic elements, structure of the information and major messages about project goals. These tools include shared standard templates, mailing lists, a Sharepoint, which is the project shared repository, and a meeting plan to monitor periodically the activities.

Due to the high number of partners located across all Europe, and to a still existing residual impact from the COVID-19 pandemic, periodical meetings will be held mainly via video conferences on a monthly basis. Physical Consortium meetings will take place twice a year, with special attention to recommendations issued by Sanitary Authorities.

Procedures and templates apply also to project reporting process including internal recording to monitor financial progress in terms of personnel effort (Person/months) every six months and the periodic report to be provided for the three official project reporting periods (M1-M12, M13-M30, M31-M42). Payments are regulated by processes defined in the Consortium Agreement signed by the SYNERGIES project partners.

In addition, the continuous risk management methodology to be applied during the whole SYNERGIES implementation has been described in detail and is accompanied by the initial Risk Registry and Contingency Plan that will be continuously monitored and assessed.

Special attention has been granted to the ethical approach and the IPR management, given the strong data-relevant nature of SYNERGIES, in order to ensure a smooth management of the SYNERGIES Energy Data Spaces.



Table of Contents

E	xeo	cuti	ve S	ummaryii				
Li	ist	of A	Acroi	nyms/Abbreviationsvi				
1		Intr	odu	ction				
	1.	1	SYN	IERGIES Project Overview				
	1.2 Del			verable Purpose and Structure9				
	1.:	3	Pos	itioning in SYNERGIES				
2		Pro	ject	management plan and structure10				
	2.	1	Proj	ect Management Plan10				
	2.	2	Man	agement structure				
		2.2.	1	Project management and coordination13				
		2.2.	2	General Assembly				
		2.2.	3	Executive Board14				
		2.2.	4	Technical Coordination15				
		2.2.	5	Exploitation and Business Innovation Coordination15				
		2.2.	6	Communication and Dissemination Activities Coordination16				
		2.2.	7	Ethics Monitoring				
	2.2.8		8	Data Management1				
		2.2.	9	Risk Management & Quality Assurance1				
		2.2.	10	WP leader1				
		2.2.	11	Partner PoC				
•		2.2.	12	Administrative and Financial Coordination				
3	~	Pro	oject	Management Implementation				
	3.	1	Deli	verables				
		3.1.	1	Official Deliverables				
	~	3.1.	2	Internal Deliverables				
	3.,	2	Proj	Templetes				
		3.2.	า ว	Templates				
		3.2.	2	Popository				
	<u>م</u>	ວ.∠. ວ	Moo	tingo				
	ა. ი	3	Dep	erting proceedure				
	3.4	4	кер ₄	Official Departs				
		3.4. 2.4	י ר	Internal Reports				
	2	5.4. 5	∠ Pov	ments				
٨	5.	0 0	ray a <i>lity</i>	Assurance Process				
4	Λ	4		Assurance Frocess				
	4.	1	Qua	inty Policy and principles				

	4.2	C	Conflict resolution			
	4.3	C	Change Management			
	4.4	C	Deliverable Preparation and Submission			
	4	1.4.1	File naming convention			
	4	1.4.2	Deliverable Submission Process			
	4	1.4.3	Deliverables Review process35			
5	F	Risk	Assesment			
	5.1	S	Scope			
	5.2	C	Continuous Risk Management Methodology			
	5.3	F	Risk Registry and Contingency Plan			
6	E	Ethio	cs approach			
	6.1	E	Ethical Aspects of Data and Artificial Intelligence51			
	6	6.1.1	Data Ethics51			
	6	6.1.2	Artificial Intelligence Ethics			
	6.2	E	Ethics Monitoring Mechanisms in SYNERGIES56			
	6	6.2.1	Ethical Considerations in SYNERGIES56			
	6	6.2.2	Compliance with the EU Privacy and Data Protection Laws			
	6	6.2.3	Organisational Mechanisms65			
	6	6.2.4	Technical Mechanisms68			
7	S	SYN	ERGIES Approach to IPR Management69			
	7.1	S	State of Play in SYNERGIES IPR Management69			
	7	7.1.1	Internal Documents Regulating the IPRs in SYNERGIES70			
	7	7.1.2	Relevant European IP Laws71			
	7	7.1.3	Key Concepts in SYNERGIES IPR Management73			
	7.2	S	SYNERGIES IPR Methodology74			
	7	7.2.1	IPR Protection in SYNERGIES75			
	7	7.2.2	SYNERGIES Data Sharing Contracts76			
8	C	Cond	clusions and Next Steps79			
R	efer	renc	es80			
A	nne	xes.				
	Anr	nex l	: Project management templates82			
	Ν	Neeti	ng Minutes including Agenda, Action list, Attendance list and Signature list82			
	F	PTI	Presentation Template85			
	D	Delive	erable Template			
Contact and Mailing List						



SYNERGIES Shaping consumer-inclusive data pathwaYs towards the eNERGy transition, through a reference Energy data Space implementation

List of Figures

FIGURE 1: PHASES OF THE SYNERGIES PROJECT MANAGEMENT LIFE CYCLE	11
FIGURE 2: SYNERGIES PROJECT MANAGEMENT STRUCTURE	12
FIGURE 3: SYNERGIES CHANGE MANAGEMENT PHASES	33
FIGURE 4: CONTINUOUS RISK MANAGEMENT IN SYNERGIES.	37
FIGURE 5: ETHICS RISKS RELATED TO AI-DRIVEN BIG DATA PROCESSING ACTIVITIES	56
FIGURE 6: THE 5-LAYER MODEL OF ETHICS BY DESIGN	66
FIGURE 7: THE EUROPEAN COMMISSION'S GENERIC MODEL FOR AI DEVELOPMENT	67
FIGURE 8: THE ENVISAGED ROLE OF DATA SHARING CONTRACTS BETWEEN THE S	SYNERGIES

List of Tables

TABLE 1: PARTNERS REPRESENTATIVES LEADING THE MANAGEMENT BODIES	13
TABLE 2: SYNERGIES OFFICIAL DELIVERABLES LIST, INCLUDING PEER INTERNAL REVIEWERS	23
TABLE 3: SYNERGIES INTERNAL DELIVERABLES LIST, INCLUDING PEER INTERNAL REVIEWERS	26
TABLE 4: SYNERGIES DELIVERABLE SUBMISSION PROCEDURE	35
TABLE 5: RISK EXPOSURE DEFINITION TABLE	37
TABLE 6: RISK DEFINITION TEMPLATE.	38
TABLE 7: LIST OF RISKS IDENTIFIED BY SYNERGIES	50
TABLE 8: IPR PROTECTION MEASURES	76



List of Acronyms/Abbreviations

Acronym/ Abbreviation	Description
AI Act	Regulation Laying Down Harmonised Rules on Artificial Intelligence
CA	Consortium Agreement
DERs	Distributed Energy Resources
DoA	Description of Action
DPO	Data Protection Manager
DSO	Distribution System Operators
EVs	Electric Vehicles
GA	Grant Agreement
HLEG	Ethics Guidelines for Trustworthy AI
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Right
LEC	Local Energy Community
РоС	Point of Contact
RES	Renewable Energy Sources
RFC	Request For Change
ТоС	Table of Contents
TSO	Transmission System Operators
WP	Work Package



1 Introduction

The main aim of Section1 is to provide a brief overview of the content structure and deliverable scope in order to present comprehensive background information regarding the SYNERGIES project for a better understanding of the contents displayed in the present document.

1.1 SYNERGIES Project Overview

The growing number of Distributed Energy Resources (DERs) connected to the network continuously expands the energy system "edge", in terms of controllability and operational complexity. The progressive decentralization, which is also accompanied by the introduction of new digitalized assets (EVs, IoT, batteries), poses significant challenges for the resilience of the system, while introducing increased uncertainty in traditional control routines, given the stochastic and intermittent character of renewable generation and the new control variables (not currently addressed in existing tools for the system management) introduced by new assets.

SYNERGIES introduces a reference Energy Data Space Implementation that will attempt to unleash the data-driven innovation and sharing potential across the energy data value chain by leveraging on data and intelligence coming from diverse energy actors (prioritizing on consumers and introducing them as data owners/ providers) and coupled sectors (buildings, mobility) and effectively making them reachable and widely accessible. In turn, it will facilitate the transition from siloed data management approaches to collaborative ones which promote the creation of a data and intelligence ecosystem around energy (and other types of) data and enable the realization of data (intelligence)-driven innovative energy services. The SYNERGIES solution will:

- value the flexibility capacity of consumers in optimizing energy networks' operation, maximizing RES integration and self-consumption at different levels of the system (community, building)
- evidently support network operators in optimally monitoring, operating, maintaining and planning their assets and coordinating between each other (TSO-DSO collaboration) for enhancing system resilience;
- create an inclusive pathway towards the energy transition, through consumer empowerment, awareness and informed involvement in flexibility market transactions;
- step on real data streams and intelligence to deliver personalized and automated features to increase prosumer acceptance and remove intrusiveness facilitate the establishment of sustainable LECs by enhancing their role with Aggregator and Business Service Provider functions;
- establish solid grounds for the creation of a new economy around energy data produced and shared across a complex value chain, in a secure, trustful, fair and acceptable manner;

In this context, SYNERGIES aims at re-conceiving data sharing against traditionally bilateral contracting applied in the energy sector and acting as multiplier of the collective data value that can be accrued, shared and traded towards achieving the resilient operation of energy systems through the coordinated optimization of their constituent components (generation, demand, storage) and the orchestrated integration with relevant sectors that can inject significant amounts of flexibility (mobility and EV charging, buildings and heating/cooling systems' control). SYNERGIES will be extensively validated in 3 large-scale demonstration sites in Greece, Spain and Denmark involving complete value chains, diverse data sources, heterogeneous energy systems/assets and spanning different socio-economic characteristics.

1.2 Deliverable Purpose and Structure

This deliverable aims at describing the Project Management principles, structure and tools that will be applied to the development of the activities of the SYNERGIES project. The goal of this document is to provide all the SYNERGIES project partners with official project management references for the execution of the project tasks, in order to achieve the project objectives and outputs in accordance with the expected timeline and the quality levels as per the contractual obligations described in the Description of the Action (DoA). Furthermore, the deliverable serves as a tool to provide the Granting Authority with an overview of the SYNERGIES management structure, including a plan for risk management and quality assurance.

The deliverable includes a comprehensive description of the project management aspects and all the measures and strategies put in place by the SYNERGIES Consortium to achieve project objectives, and it is structured as follows:

- Section 2 describes the Project Management principles and plan providing detailed information about its structure, with an explanation of the set of entities and management operational bodies identified to ensure a solid implementation of the project activities.
- Section 3 provides an overview of the tools (standard templates, mailing list, repository) and procedures (meetings, reporting, payments) envisioned by the SYNERGIES Project Management process to ensure a smooth execution and an efficient monitoring of activities implementation.
- Section 4 describes the quality assurance processes envisioned by the Project Management (conflict resolution, change management, standard procedure for Deliverable preparation and submission) in order for the project results to be in line with the contractual obligations.
- Section 5 includes the risk management strategy, with a detailed description of the methodology, the registry and the contingency plan.
- Section 6 provides an overview of the SYNERGIES ethical approach, management and monitoring with regards to the development and use of the Energy Data Spaces platform.
- Section 7 specifies the issues linked to IPR, which lays the foundation for exploitation tasks
- Section 8 includes the closing remarks of the document, with a specific reference to the next steps concerning the updates to the Project Management plan described in this document, in line with the continuous iteration and adaptation principle that characterises the overall SYNERGIES approach.

1.3 Positioning in SYNERGIES

This document describes the action of WP1 "SYNERGIES Project Management", which cuts across all the other WPs (WP2-WP7) and activities, providing horizontal references for governance and methodologies to ensure the consistency and the quality of the project results. All the project activities and production of documents and materials will be carried out according to the share of responsibilities and the procedures set out in the present document.

The present document contains references to:

- the project Grant Agreement, which describes in detail the actions that will be carried out throughout the project and the expected results
- Consortium Agreement, which provides the guidelines and regulations that serve as a basis for the definition of project governance bodies and management procedures.

2 Project management plan and structure

Section 2 provides a complete overview of the project management methodology that will be applied to the SYNERGIES project, in order to guarantee an efficient collaboration of partners to achieve the project goals concretely and on time. The Project management plan and its structure will be hereby explained, including detailed information on the agile approach adopted in the development of the project activities and the specific operational bodies that will collaborate to ensure a smooth and successful project development.

As mentioned, the project management plan is characterized by an agile project management plan which envisions 6 phases for an efficient monitoring of project execution and a prompt revision of the activities in view of risks and problem management. Such efficient monitoring and coordination of activities includes the establishment of specific entities that oversee the management of activities related to the core elements of SYNERGIES. These entities include the general project management and coordination, the technical coordination, the exploitation and business innovation coordination, the communication and dissemination activities coordination, ethics monitoring, data management, risk management and administrative and financial coordination. In addition to these entities, specific bodies have been defined to oversee the overall implementation of activities, such as the WP leaders, and to make decisions over important matters impacting the project execution, namely the General Assembly and the Executive Board.

The project management approach and all the entities and bodies are described in the following sections.

2.1 Project Management Plan

SYNERGIES involves a complex ecosystem of entities (partners) with different competences and roles within the project. In order to have an efficient and successful delivery of all activities, the SYNERGIES project management has adopted an agile approach, based on a life cycle divided into 6 distinct phases: *conceptualization, planning, implementation, monitoring, adaptation* and *closure*. The adoption of such phases provides a strategy to monitor that the project proceeds as planned. The planning, implementation and monitoring phases are linked to each other in a circular process, in which the outcomes of a step act as the input for the following one. This allows for continuous iteration and adaptation of the activities and the outputs. The monitoring phase ensures that in cases where changes are needed, corrective actions can be implemented to ensure that the project quickly adapts the modifications required to meet the Gantt timeline and deadlines. This loop continues until there are no additional adjustments and all project activities and deliverables have been successfully completed. The project management life cycle phases are defined as follows:

- Phase 1 *Conceptualization*: in this phase the work plan for execution is designed, defining the work packages and their interconnections, including the respective tasks to be implemented. The Partners' Point of Contacts (PoC) are identified.
- Phase 2 *Planning*: this phase envisages the development of the detailed work plan and guidelines for project coordination and monitoring, in order to achieve the project's goals efficiently in terms of time and resources.
- Phase 3 *Implementation*: the concrete development of project activities takes place, according to what was established in the previous phases. The implementation is led through methodical activities of consortium coordination, which guarantee the production of the foreseen internal and external progress reports at technical or financial level, and the (official and internal) project deliverables.
- Phase 4 *Monitoring*: it includes key activities to assess the project progress and consequently highlights the achievements and obstacles encountered. Monitoring is essential to detect any emerging deviations from the work plan: project partners can enact corrective measures to ensure the anticipated project quality level.



- Phase 5 *Adaptation*: thanks to the inputs that have emerged during the monitoring phase, the project partners will be able to reassess the initial assumptions and identify appropriate adjustments to project processes, strategies and methods through interventions and corrective measures that will contribute to deliver high quality results.
- Phase 6 *Closure*: as a result of the previous phases, all planned goals have been achieved, all deliverables have been submitted, and all administrative tasks have been completed. This phase includes the project evaluation process by the European Commission, which assesses the output and outcomes of the project in comparison to the actions and goals laid out in the Grant Agreement.



Figure 1: Phases of the SYNERGIES Project Management life cycle

2.2 Management structure

SYNERGIES has put in place an efficient management structure to address the challenge of coordinating a project with a high number of partners with different competences and working in dislocated locations across Europe. The SYNERGIES project management structure is based on the best practices from the coordinator and partners' long experience in the management of innovation projects. The goal of the structure is to be able to provide enough flexibility as needed by an innovation project, while at the same time ensuring the high quality of the project results.

The management structure identifies three governance levels (European, project and WP level) that contribute to an efficient monitoring of the project progress and provide a clear accountability plan for the development of the activities.

At the European Level, the European Commission periodically assesses the progress of the project and the fulfilment of its contractual obligations. At project level, a set of entities and management operational bodies have been identified to ensure a smooth project coordination and a continuous monitoring of the project activities in terms of ethics, data management, technical coordination, risk management, administration and financial resources, exploitation and dissemination.

Form the operational point of view, the work to be done within SYNERGIES is structured into a set Work Packages (WPs). Each WP is led by a WP leader, selected among the project partners according to their competences and expertise. This ensures an equal workload allocation and an efficient development of the project activities. The PoCs of the partners involved in each WP report their work progress to the WP leader, for a smooth coordination and execution of the specific tasks. In order to provide the WP leader with the different information needed, two types of PoCs are identified for each partner: Technical PoC and Finance & Administration PoC.



The management structure is shown in detail in the following picture.



Figure 2: SYNERGIES project management structure



Selected project partners are in charge of the project management bodies, based on their competences and on their role within the project. The complete list of the partners leading each management body is shown in the following table.

Management Body	Partner
Project management and coordination	тхт
Technical Coordination	SUITE5
Exploitation and Business Innovation Coordination	тхт
Dissemination Activities Coordination	тхт
Ethics Monitoring	ALBV
Data Management	тхт
Risk & Quality Management	SUITE5
Administrative and Financial Coordination	ТХТ

Table 1: Partners representatives leading the management bodies

2.2.1 Project management and coordination

The Project Coordinator is responsible for the overall management and coordination of the project and, is also accountable for the project direction and success. Moreover, the Project Coordinator is the main project representative and the formal communication point with the EC and other bodies.

Specifically, as described in the Consortium Agreement, the Project Coordinator role is to:

- ٠ monitor compliance by the Parties with their obligations under this Consortium Agreement and the Grant Agreement;
- keep the address list of Members and other contact persons updated and available;
- collect, review to verify consistency and submit reports, other deliverables (including financial statements and related certifications) and specific requested documents to the Granting Authority;
- transmit documents and information connected with the Project to any other Parties concerned:
- administer the financial contribution of the Granting Authority and fulfil the financial tasks described in Section 7.2 of the Consortium Agreement;
- provide, upon request, the Parties with official copies or originals of documents that are in the sole possession of the Coordinator when such copies or originals are necessary for the Parties to present claims;
- chair the meetings and monitor the implementation of decisions made during these meetings.

The SYNERGIES project coordination and management will be carried out by TXT e-solutions SpA (TXT).

2.2.2 General Assembly

As per Consortium Agreement, the General Assembly is the ultimate decision-making body of the consortium. It shall consist of one representative of each partner, and it is chaired by the Project Coordinator. The General Assembly will meet twice a year, approximately in Spring and in Autumn, and will be held physically at different partners' premises on a rotating basis. Extra meetings will be scheduled when needed. The hosting partner can give the opportunity to partners that were unable to travel to attend the meeting via teleconference.



The Project Coordinator will share the meeting's agenda in due time, and partners will be able to add their input items. Minutes of the meetings will be produced by the coordinator, and consequently shared with the project consortium.

Concerning decisions, the General Assembly can deliberate upon:

- Content, finances and intellectual property rights
 - Proposals for changes to Annexes 1 and 2 of the Grant Agreement to be agreed by the Granting Authority
 - Changes to the Consortium Plan
 - Modifications or withdrawal of Background in Attachment 1 of the CA (Background Included)
- Additions to Attachment 3 of the CA (List of Third Parties for simplified transfer according to Section 8.3.2) Evolution of the consortium
 - Entry of a new Party to the Project and approval of the settlement on the conditions of the accession of such a new Party
 - Withdrawal of a Party from the Project and the approval of the settlement on the conditions of the withdrawal
 - $\circ~$ Identification of a breach by a Party of its obligations under this Consortium Agreement or the Grant Agreement
 - Declaration of a Party to be a Defaulting Party
 - o Remedies to be performed by a Defaulting Party
 - Termination of a Defaulting Party's participation in the Project and measures relating thereto
 - Proposal to the Granting Authority for a change of the Coordinator
 - Proposal to the Granting Authority for suspension of all or part of the Project
 - Proposal to the Granting Authority for termination of the Project and the Consortium Agreement Appointments

On the basis of the Grant Agreement, the appointment is necessary for Executive Board Members.

Each partner in the meeting will have one vote. The presence of two-thirds (2/3) of the partners is required for the General Assembly to deliberate and decide validly in meetings (quorum). Decisions will be taken by a majority of two-thirds (2/3) of the votes cast.

2.2.3 Executive Board

As described in the CA, the Executive Board acts as the supervisory body for the execution of the Project, which shall report to the General Assembly. The Executive Board is composed by the Project Coordinator, the Technical Coordinator and the WP leaders, and its meetings are chaired by the Project Coordinator.

The Executive Board will meet via videoconference when considered appropriate upon request by any Executive Board member.

The Executive Board will:

- Monitor periodically the effective and efficient implementation of the Project to assess the compliance of the Project with the Consortium Plan and, if necessary, propose modifications of the Consortium Plan to the General Assembly. In this regard, the project partners have established recurring Internal Deliverables, which will serve to monitor the progress of activities, as described in section 3.1.2.
- Be responsible for the proper execution and implementation of the decisions of the General Assembly.
- Prepare the meetings, propose decisions and prepare the agenda of the General Assembly.



• Support the Coordinator in preparing meetings with the Granting Authority and in preparing related data and deliverables.

The Executive Board is composed by the following partners :TXT, Suite5, ICCS, ETRA and HEDNO.

2.2.4 Technical Coordination

The Technical Coordinator is responsible for properly steering, managing and monitoring all technical aspects of the SYNERGIES project. The Technical Coordinator will be practically in charge of defining and conveying the underlying SYNERGIES vision and strategic orientation from a technical perspective while ensuring that all project activities are aligned to it. In collaboration with the Project Coordinator and the Exploitation and Business Innovation Manager, the Technical Coordinator will guarantee that the SYNERGIES results go beyond the state-of-the art, follow the market trends and meet the actual user needs/requirements in an efficient manner, with clear added value and benefits.

The Technical Coordinator will oversee the technical developments across all technical WPs (WP2-WP5), organize bi-weekly technical meetings in order to ensure cross-WP alignment of all results and continuously monitor the progress performed. With the support of the WP2-WP3-WP4 Leaders, the Technical Coordinator will define the specifications and design/implementation principles and will be responsible for the consistency of all project results throughout the different project implementation phases.

In addition, the Technical Coordinator will define the fine-grained technical plan with detailed activities and deadlines at task level in order to ensure that the expected official and internal deliverables (defined in Section 3.1) will be delivered on time and with the expected high quality. Once the development activities in WP3-WP4 start, the Technical Coordinator will track progress against the defined development and integration plan and will be in close collaboration with the Project Coordinator, the WP leaders and the Risk & Quality Manager to timely address any deviation or issue that may arise.

The Technical Coordination activities will be carried out by Suite5.

2.2.5 Exploitation and Business Innovation Coordination

The Exploitation and Business Innovation Coordinator will be in charge of aligning the technical development of the Energy Data Space platform with the business exploitation, to ensure a proper uptake of project results by the market. He will coordinate the exploitation tasks and will work in close collaboration with the Technical Coordinator and will be also responsible for designing a concrete strategy that will be launched to carry forward the exploitation and operation of the platform. Driven by its innovation nature, SYNERGIES is clearly aligned with industry and market trends and has the potential to impact the market shortly after project completion by offering a reference implementation for a common European Energy Data Space.

The Exploitation and Business Innovation activities will be carried out in WP6, along with the communication and dissemination activities. This is due to the fact that dissemination is expected to actively support and promote the exploitation and future success of the project outputs. Exploitation is tightly connected to several dissemination actions that implicitly and explicitly contribute to the timely commercialization of the project results, inside and beyond the consortium.

Therefore, SYNERGIES will invest in the mobilization of highly effective dissemination, communication and engagement means to reach and engage with energy data value chain stakeholders for codesigning and co-creating innovative solutions that can create immediate market impact. This approach will aim at paving a secure path towards the commercial exploitation of the project results. The exploitation potential of the project will be further reinforced through targeted contributions to policy makers (policy briefs) and standardization bodies (standardization punch-lists) to encapsulate



validation findings in emerging regulations and interoperability roadmaps, thus further enhancing the commercial potential and market positioning of the project.

The SYNERGIES Exploitation and Business Innovation Coordinator will be TXT.

2.2.6 Communication and Dissemination Activities Coordination

The Communication and Dissemination Coordinator will be responsible for all dissemination and communication activities and direct interaction with mass media and energy sector stakeholders, as well as for the creation of a common visual identity and the management of the project website and the social media structure, content and functionalities. Finally, the Communication and Dissemination Coordinator will ensure that the Project achieves excellent outreach through public events, scientific publications, and presentations. In addition to these traditional communication and dissemination means, the SYNERGIES communication and dissemination strategy envisions Living Lab Activities, which are key to reach out to end-users and external stakeholders and involve them in all phases of the project implementation, provide them with early access to the project results, and involve them in an iterative process of co-creation and continuous validation of the projects result.

For all its dissemination activities, SYNERGIES will adopt the priority principles of open science set out by the European Commission. This applies both to publications and preliminary designs of the energy solutions produced by the project.

Complete and comprehensive details about the SYNERGIES communication and dissemination strategies and tools are described in deliverable D6.1 Dissemination, Communication and Engagement Plan.

Communication and Dissemination Activities are included in WP6, and they will be coordinated by TXT.

2.2.7 Ethics Monitoring

Given the intensive use of data which SYNERGIES envisions to populate an Energy Data Space so as to provide data-driven services, ethics principles are of foremost importance and need to be carefully given attention to, as they are of horizontal relevance for all the activities envisioned to be undertaken by the project. Therefore, a specific entity has been established to monitor SYNERGIES' compliance to these principles.

The two main ethical considerations that arise in SYNERGIES are related to:

- ٠ data ethics: the principle prescribes that data sharing is conducted in accordance with the principles of ethical data sharing. SYNERGIES involves the collection of prosumer-related data, which will include among others, personal data. Therefore, it is crucial to ensure that individuals involved are able to exercise their fundamental rights, placing them at the centre of the innovative initiative by enabling individual control, transparency, accountability, and equality in how data is utilised within the project. This will allow for the creation of a trusted environment and for data sharing to adhere to regulatory framework on data protection.
- Al ethics: trustworthiness is a prerequisite for individuals and societies to develop, deploy and use AI systems. It is Important that SYNERGIES comply with such prerequisite given the AI elements involved in the project, namely the machine learning models and various reasoning techniques that will be tested and implemented within the project. In order to have a trustworthy AI, SYNERGIES shall take into account the principles of the ethical AI, such as Respect for human autonomy, Privacy & Data Governance, Fairness, Prevention of harm, safety and well-being, Transparency and Explicability, Accountability by design, control and Oversight.

The design and use of appropriate tools to guarantee ethics monitoring and compliance will be carried out by ARTHUR'S LEGAL BV.

2.2.8 Data Management

Due to the strong data-relevant nature of SYNERGIES, Data Management has a prominent role in the project. Data management will tackle the management lifecycle for the data to be collected, processed and/or generated by the SYNERGIES project, along the FAIR (making research data Findable, Accessible, Interoperable and Re-Usable) principles and the corresponding roles of partners and resources to be utilized. More specifically, data management activities will ensure that the following aspects are defined:

- handling of research data during & after the project (use and re-use of data);
- what data will be collected, processed and/or generated;
- which methodology & standards will be applied;
- whether data will be shared/made open access;
- how data will be curated & preserved.

Such information will be included in a separate deliverable *D1.2 Data Management Plan*. Updates of the DMP will be provided as part of the Periodic Management Reports. Moreover, the data manager will also act as Data Protection Officer (DPO).

Data Management activities will be coordinated by TXT.

2.2.9 Risk Management & Quality Assurance

The Risk and Quality Manager is allocated with a dual role, including, on the one hand, the implementation of the quality procedures determined in the present Project Management Plan (Section 4) and the verification of the high quality of the project results; and on the other hand, the definition and application of the continuous risk management methodology and the control of the Risk Management Plan (Section 5). The Risk and Quality Manager is responsible for raising awareness for any observed or anticipated deviations (from a quality perspective) and for any early indications for the materialisation of a risk (described in the Risk Registry) at the WP level and/or the project level.

The risk management and quality assurance activities will be carried out by Suite5.

2.2.10 WP leader

Each WP has a clearly identified leader responsible for coordinating the work within the WP in order to ensure its smooth and timely execution. The WP leader is also responsible for stimulating the interaction among the various partners involved and monitoring progress of Tasks within the WP, as well as for inter-WP liaison. Each task has a leader too, who reports to the respective WP leader. Specifically, the WP leader responsibilities are:

- Orchestrate and supervise multiple tasks and activities within the WP.
- Propose work plan modifications to the Executive Board, if necessary.
- Inform the Project Manager about the task progress of the WP.
- Call progress meetings, if needed, to inform all WP leaders, the Technical Coordinator and the Project Coordinator about important issues that may have arisen.
- Contribute to project deliverable preparation and ensure their high-quality level.
- Report to the Executive Board and General Assembly.

The SYNERGIES WP leaders are: TXT, ICCS, Suite5, ETRA, HEDNO.

2.2.11 Partner PoC

To ensure that the Consortium internal communication reaches all the partners efficiently, a Point of Contact (PoC) has been selected for all Consortium members. PoCs are the main representatives for their organisation, to whom the Project Coordinator refers to. Moreover, in order for communications to target the correct people within the partners' organisations and avoid an excessive exchange of



emails which could create confusion, different PoCs have been identified, based on their specific role and competencies:

- Administrative and Financial PoC, who receives communication related to administrative i. *matters* (financial statements, signature of contracts, payments, etc.)
- ii. Technical PoC: who receives communication related to project activity execution

As described in section 3.2.2, different mailing lists have been created based on this role distinction, with the aim of targeted communication distribution.

The complete list of the PoCs (Administrative & Financial and Technical) for each project partner is accessible on the shared repository and it will be updated shall any change of staff occur. The template for the list of PoCs has been attached to the present deliverable as an annex.

2.2.12 Administrative and Financial Coordination

Administrative and financial coordination activities ensure a punctual and smooth fulfilment of financial and administrative issues, namely:

- the establishment and maintenance of financial records
- the correct submission of cost statements by all project partners,
- following-up on EC payments;
- distribution of partners' financial contribution shares according to CA agreed rules. •

Within the SYNERGIES project, several tools have been designed to support the coordination of such activities: different partners mailing lists, a shared repository for the official documents, the templates to collect the relevant information, the reporting procedures and a meetings schedule to ensure that all the partners are properly informed and aligned on the tasks.

The Project Coordinator (TXT) is in charge of ensuring the correct delivery of the above-mentioned contractual obligations.

3 Project Management Implementation

Section 3 aims to give a comprehensive overview of the set of project management tools and procedures envisioned by the SYNERGIES project, which support the efficient coordination and monitoring of the project activities execution, ensuring that it is in line with the expected quality level.

The foremost instrument that supports the project management implementation is the Deliverables. Deliverables represent the progressive results of the main elements of project in each WP. In addition to the Official Deliverables enlisted in the project's Grant Agreement, the project consortium has established a set of Internal Deliverables to track more closely the progress of activities and guarantee their smooth delivery.

Moreover, the SYNERGIES project management is supported by a set of tools aimed at ensuring a smooth collaboration among project partners and that project contents are produced consistently and stored efficiently.

The next sections will give an overview of the above-mentioned tools and procedures set out by SYNERGIES to put in place a solid project management throughout the project lifetime.

3.1 Deliverables

The Project plan foresees a number of deliverables that will be submitted to the European Commission to report both the planning of project activities and the final results, including periodic updates and reviews of said outcomes. Each deliverable is associated to a Beneficiary which is fully responsible for the deliverable quality and timely submission and is required to maintain adequate control of the participants' contributions. The procedures to submit and review a deliverable are described in sections 4.4.2 and 4.4.3.

In addition, all project partners have agreed to create periodic "internal deliverables", which will allow for a more efficient tracking of the progress of project activities.

All deliverables (both official and internal) are subject to the review of internal peer reviewers selected among the project partners, who will revise the documents in order to guarantee they reach an adequate quality level.

A complete list of the Deliverables (Official and Internal) can be found in the next sub-sections.

3.1.1 Official Deliverables

In order to track and report the concrete results of SYNERGIES, a list of WP specific deliverables (D) has been drafted. The list counts 16 official deliverables. Each deliverable has a specific deadline based on the project GANTT. The responsible for each deliverable has been identified among the partners involved in the specific WP, according to the scope of the deliverable and considering a fair workload distribution. In order to guarantee that the deliverables contents are complete and consistent with the project's goals and scope, an internal double-review system was set-up. To ensure transparency, two internal reviewers have been identified for each deliverable, allocating the workload equally among the partners. The dissemination level of the deliverables (public or confidential) is specified based on each deliverable's scope.

A complete list of the official deliverables, including the assigned internal reviewers, is presented below:



	SYNERGIES Deliverables List								
Deliverable n.	WP n.	Title	Description	Lead Beneficiary	Туре	Dissemination Level	Due date M	Internal reviewer #1	Internal reviewer #2
D 1.1	WP1	Project Management Plan	Includes all project management procedures and templates, a detailed technical implementation plan, the risk assessment and ethics monitoring frameworks	1 - TXT	R — Document, report	PU - Public	3	ICCS	HEDNO
D6.1	WP6	SYNERGIES Dissemination, Communication and Engagement Plan	A roadmap for the setup of the SYNERGIES living lab and the planning of the dissemination, communication and engagement activities of the project. It involves also the delivery of the initial communication material of the project.	1 - TXT	R — Document, report	PU - Public	3	Π	COEN
D1.2	WP1	Data Management Plan	Includes the initial DMP along the FAIR principles and the corresponding roles of partners and resources to be utilized. It is provided as a separate deliverable due to the strong data-relevant nature of the project. Updates of the DMP will be provided as part of the Periodic Management Reports.	1 - TXT	0 — Other	PU - Public	6	ALBV	PI
D2.1	WP2	1st version of SYNERGIES Requirements and Detailed Architecture Design	Report on the end-user and business requirements (including an analysis of the socio-economic and regulatory barriers) and the project MVP, accompanied by the corresponding technical design and specifications of the individual components and integrated SYNERGIES solution.	2 - ICCS	R — Document, report	PU - Public	12	SUITE5	DTU



D3.1	WP3	SYNERGIES Energy Data Space Release 1.00	First version of the Integrated SYNERGIES Energy Data Space in preparation for the 1st demonstration phase of the project	8 - Suite5	O — Other	PU - Public	18	MAGGIOLI	ETRA
D7.1	WP7	Intermediate Report on Interoperability Demonstration and Liaison activities	Report on the preliminary activities performed in collaboration with sister projects towards the definition of Fundamental Requirements for a common European Energy Data Space, the validation of Energy Data Spaces Integration and Interoperable Data Exchange and the interactions performed with relevant initiatives and existing data platforms/ datahubs.	1 - TXT	R — Document, report	PU - Public	18	PI	ТХТ
D6.2	WP6	SYNERGIES Dissemination, Engagement and Exploitation Plan	Includes the reporting of dissemination, communication and engagement activities, together with their updated plan. It also involves the preliminary exploitation strategy for the SYNERGIES Energy Data Space and individual KERs. Finally, a first version of the SYNERGIES business models will be included, in preparation for their assessment during demo activities.	1 - TXT	R — Document, report	PU - Public	20	FORNES	BEOF
D4.1	WP4	Release of the Energy Services, Applications and Marketplace	Initial release of the energy services/ applications and marketplace for the 1st phase of the demonstration activities	10 - ETRA	0 — Other	PU - Public	22	UOP	UBITECH



D2.2	WP2	Final version of the SYNERGIES Requirements and Detailed Architecture Design	An updated version of D2.1 properly revising the requirements & architecture considering findings of the pre-validation phase.	2 - ICCS	R — Document, report	PU - Public	28	ROESOFT	IES
D5.1	WP5	SYNERGIES Validation Framework and Demonstration Management Plan	Includes a detailed report the pre- validation and performance verification tests of the project results, together with the audits, procurement and deployment performed in the demonstration sites. It also includes the evaluation methodology to be applied, the validation scenarios and the overall plan for the execution of the demonstration activities of the project.	14 - UOP	R — Document, report	PU - Public	28	SUITE5	TENO
D5.2	WP5	SYNERGIES Intermediate Evaluation and Impact Assessment Report	Consists in the assessment of the impact achieved and findings observed during the 1st demonstration phase of the project.	13 - VTT	R — Document, report	PU - Public	35	CUERVA	VTT
D3.2	WP3	SYNERGIES Energy Data Space Final Release	Final version of the SYNERGIES Energy Data Space, incorporating findings from the 1st demo phase, towards validation in the 2nd phase of the demonstration activities	8 - Suite5	0 — Other	PU - Public	36	ETRA	ICCS
D4.2	WP4	Final Release of the Energy Services, Applications and Marketplace	Final version of the applications and marketplace, incorporating findings from the 1st demo phase, towards their validation in the 2nd phase of the demo activities.	10 - ETRA	0 — Other	PU - Public	36	UBITECH	IES



D5.3	WP5	SYNERGIES Final Evaluation and Impact Assessment Report	Report on the assessment of the impact achieved during the 2nd demonstration phase of project, including a consolidation of lessons learnt, relevant policy and standardization recommendations and planning for the scaling up and replication of the project results	13 - VTT	R — Document, report	PU - Public	42	ТХТ	ΙΡΤΟ
D6.3	WP6	SYNERGIES Business Innovation Plan	Elaboration on the SYNERGIES Exploitation Strategy and Business Innovation Plan with regards to the SYNERGIES Energy Data Space as the core outcome of the project. The report will also provide updates of the individual exploitation plans and new business models for the energy sector actors, while reporting on the implemented dissemination, communication and engagement activities and defining an associated plan for the post-project period to support the exploitation of the SYNERGIES Energy Data Space	1 - TXT	R — Document, report	SEN - Sensitive	42	VTT	Π
D7.2	WP7	Final Report on Interoperability Demonstration and Liaison activities	Update of D7.1 reporting on the latest collaboration activities performed and lessons learned	8 - Suite5	R — Document, report	PU - Public	42	HEDNO	CIRCE

Table 2: SYNERGIES official deliverables list, including peer internal reviewers

3.1.2 Internal Deliverables

In order to guarantee a more efficient tracking of the progress project activities, the project partners have agreed to create periodic "internal deliverables", serving as preparatory documents or as updated progress reports of the official deliverables, depending on whether the document is prepared *before* or *after* the official due date of the deliverable submission. A total number of 9 internal deliverables is scheduled. The planning of these documents has been established based on the activities schedule of each WP. Moreover, they are scheduled considering an adequate time distance from the official deliverables, in a way not to be excessively close or far from these deadlines. The beneficiary in charge for the official deliverables will be accordingly in charge of the internal ones. Finally, as for the official deliverables, the same ratio of transparency and equal workload allocation have been applied in the identification of the two internal peer reviewers for the internal deliverables.

The internal deliverables will be available upon request to the EC Project Officer for information and better project monitoring from both beneficiaries and Grant Authority perspective. Since the goal of these documents consists in ensuring an efficient and ongoing follow-up of project activities, the internal deliverables will not be subjected to upload on the ECAS portal nor to any official approval procedure from the EC.

Here below the complete list of internal deliverables approved by the project partners, with the respective internal reviewers:



SYNERGIES Internal Deliverables List										
Deliverable n.	WP n.	Title	Description	Correlation to Official Deliverables	Lead Beneficiary	Туре	Dissemination Level	Due date M	Internal reviewer #1	Internal reviewer #2
ID2.01	2	Internal Deliverable - Draft Use Cases and Requirements	Progress report on activities carried out in T2.1 - 2.2 - 2.3: Draft Concept (T2.1), Draft Use Cases (T2.2), Draft Business & User Requirements (T2.2), Draft Barrier Analysis (T2.3)	Preparatory to D2.1	2 - ICCS	R — Document, report	In - Internal	6	ALBV	HEDNO
ID2.02	2	Internal Deliverable - Updated concept, use cases, requirements, architecture	Progress report on activities carried out in T2.1 - 2.2 - 2.3 - 2.4: update of the concept, use cases, reqs, architecture	Update of D2.1 and preparatory to D2.2	2 - ICCS	R — Document, report	In - Internal	24	Ы	VTT
ID3.01	3	Internal Deliverable - Draft CIM Network, Detailed Development Plan	Progress report on activities carried out in T3.1 (CIM Network Approach and standards definition of sectorial data models) and development roadmap	Preparatory to D3.1	8 - Suite5	R — Document, report	In - Internal	12	CIRCE	ΙΡΤΟ
ID3.02	3	Internal Deliverable - Updated Development Plan	Progress report on activities carried out in T3.1 - 3.2 - 3.3 - 3.4 - 3.5 - 3.6: Updated Network of Sectorial Data Models, Scalability / stress testing of the initial release of the SYNERGIES Energy Data Space, Update of the Development roadmap	Update of D3.1 and preparatory to D3.2	8 - Suite5	R — Document, report	In - Internal	28	TENO	ICCS
ID4.01	4	Internal Deliverable - Detailed Development Plan	Definition of WP4 development roadmap	Preparatory to D4.1	10 - ETRA	R — Document, report	In - Internal	12	UOP	CUERVA
ID4.02	4	Internal Deliverable - Updated Development Plan	Progress report on activities carried out in T4.1 - 4.2 - 4.3 - 4.4 -4.5: Finalisation of integration activities with actual demo data for the 1st trial phase (WP5) - Fully functional Digital Twins & Energy Apps	Update of D4.1 and preparatory to D4.2	10 - ETRA	R — Document, report	In - Internal	28	тт	DTU
ID5.01	5	Internal Deliverable - Early Demonstration Profiling (Data Assets, Energy Assets)	Progress report on activities carried out in T5.1: Data Landscaping Inputs from demo sites, Asset Landscaping	Preparatory to D5.1	14 - UOP	R — Document, report	In - Internal	7	UBITECH	MAGGIOLI



SYNERGIES Shaping consumer-inclusive data pathwaYs towards the eNERGy transItion, through a reference Energy data Space implementation

ID5.02	5	Internal Deliverable - Early Demonstration Plan (Demo Cases Refinement, Roadmap)	Progress report on activities carried out in T5.1: Updated Data Landscaping Inputs from demo sites, Updated Asset Landscaping, Draft gap analysis in demo sites & WSN configuration specifications, detailed equipment procurement plan	Preparatory to D5.1	14 - UOP	R — Document, report	ln - Internal	12	ETRA	SUITE5
ID5.03	5	Internal Deliverable - Final version of the Demonstration Plan (Demo Cases Refinement, Roadmap) & Evaluation Framework	Progress report on activities carried out in T5.1 - 5.2 - 5.3 - 5.4 -5.5: Draft evaluation framework, Testing & pre- pilot validation of the SYNERGIES Energy Data Space (WP3) - initial list of tests for the WP4 components, Planning of the Scalability / Stress testing activities. Detailed Data Uploading Activities Roadmap	Preparatory to D5.1	14 - UOP	R — Document, report	ln - Internal	18	IES	тхт

Table 3: SYNERGIES internal deliverables list, including peer internal reviewers



3.2 Project Management Tools

A set of project management tools has been developed to allow an efficient collaboration among the project partners towards the project's outputs, through targeted internal communication, an easy-toaccess shared documentation space and standardized templates for a coordinated internal communication and structured data collection.

3.2.1 Templates

Standardized and coordinated templates are essential for a twofold reason:

- i. It allows the project to have a coherent branding, which contributes to the project's identity and its immediate recognition
- ii. It provides partners with a consistent structure for input collection. This is key to carry out an efficient monitoring of data of a different nature.

More specifically, different templates have been developed by the Project Coordinator and shared on the official repository (see section 3.2.3) with the project partners, namely:

- Power Point Presentation Template: an official presentation template branded with the SYNERGIES project identity (logo, colours) to be used at internal partners meetings and at external events and conferences where partners present SYNERGIES and its results.
- Deliverable Template: a common Microsoft Word template has been created for partners in ٠ charge of the creation of Deliverables. This contributes to a coordinated organization of contents and a consistent presentation of the project results to the Granting Authority.
- Effort Reporting Table Template: a Microsoft Excel template table has been created for all partners to report their expenditure in terms of personnel effort (Person/months). This allows for an efficient tracking of personnel effort spent vs. planned throughout the project lifetime and will facilitate the sharing of solid and consistent data for Periodical and Final Reporting with the Granting Authority.
- Meeting minutes (including agenda, action list, attendance and signature list): materials accessible to all partners

The abovementioned templates are attached as annexes at the end of the present deliverable.

3.2.2 Mailing list

Mailing lists have been established from M1 to support information exchange among partners. In order for communications to target the correct people within the partners' organisations, different mailing lists have been created, based on the different group of activities related to the project scope:

- A General mailing list, which includes all the staff involved in the project within the various partners.
- An Administrative mailing list, for internal communications related to administrative matters • (financial statements, signature of contracts, payments, etc.), which targets the partners' administrative staff involved in the project (Administrative and Financial PoCs).
- A Technical mailing list, for internal communications related to project activity execution which targets the partners' technical staff involved in the project (Technical PoCs).
- A mailing list dedicated to Demonstrators, assigned to share communications related to demo sites activities.

Members' subscription is managed and maintained by the Project Coordinator. The updated subscription list for all the mailing lists is available to partners in the project repository. Consortium partners are responsible to inform the Project Coordinator whether any modification of their representatives is needed.

3.2.3 Repository

The Project Coordinator has created and put at the disposal of partners a shared online repository. The repository is based on Microsoft SharePoint on cloud Office 365 infrastructure. Access to the shared repository is granted by the Project Coordinator according to the General mailing list. The major repository folders are:

• 01_Contractual Documents contains all official documents including signed Grant Agreement, signed Consortium Agreement, proposal as well as all submitted deliverables and review reports.

• 02_Administration contains administrative documents like cost statement, payment documents, etc.

• *03_Meetings* contains one folder for each meeting including agenda, logistic information, minutes, PPTs and any other material connected to the meeting.

• 05_WPs each WP has its own folder. Each WP leader can self-organize the sub-folder structure and the material managed. It is required to keep a deliverable folder where to store connected material, contributions, the editing versions, peer-review and the final word version of the submitted deliverable which will also be uploaded in the 01_Contractual Documents.

• 10_Material&Templates contains project documentation useful for internal purposes such as templates, deliverable and milestone list, dissemination material like the project logo in different formats and the official project presentation.

3.3 Meetings

In order to create synergies, cooperate and organize activities, periodic meetings will be scheduled at Consortium level, WP level and for activity clusters (such as Technical activities). Section 6.2 of the SYNERGIES CA includes the specific procedures to organize meetings and the voting rules.

In order to guarantee an efficient and transparent tracking of activities and timely activities execution, the project coordinator, in agreement with the project partners and according to the rules set out by the CA, has suggested the following meeting schedule:

- 2 physical GAs per year, one every six months, at different partners' premises on a rotating basis.
- Executive board meetings organized when needed, to focus on more strategic aspects of WP direction and progress.
- Monthly meetings at consortium level, planned every third Wednesday of the month to ensure a smooth coordination and periodical monitoring of the project's progress. These meetings are held virtually.
- Technical meetings (video conferences) held bi-weekly, to discuss the development of technical activities with the technical PoCs and the rest of the relevant staff from the partners involved.
- Meetings at WP level held to monitor the progress of activities within the WP and at task level. The WP leader can decide when to schedule such meetings according to necessity (monthly, bi-monthly, etc).

The chairperson of the meeting will give written notice of a meeting to each participant as soon as possible and no later than the minimum number of days preceding the meeting as indicated in the article 6.2.2.2 of CA.

The Coordinator (or the chairperson of the meeting, if different from the Coordinator, e.g. in WP meetings) will prepare and send each participant an agenda no later than the minimum number of days preceding the meeting as indicated in the CA (article 6.2.2.3).

After the meetings, the chairperson prepares and shares the meeting minutes, which include the action points, the attendance list and the signature list (the relevant templates provided to the partners by the Coordinator are accessible on the shared Repository).

3.4 Reporting procedure

In order to monitor and give an update of the project execution to the Granting Authority, the Project Coordinator is responsible for periodical collecting the relevant information (in form of reports) from the different partners. Project reporting is a responsibility of the whole Consortium and every partner must be actively involved in it. SYNERGIES envisions two different reporting procedures, with a different timing and different objectives: official reports and internal reports, which will be described in the following sections. Specific templates will be provided to the partners for both reporting procedures.

3.4.1 Official Reports

Official reports are aimed at updating the European Commission on the project execution, providing information on the progress of activities compared to what described in the Description of Action (DoA).

There are three official reporting periods in SYNERGIES. The official reporting periods end with the submission of a periodic report to the EC.

The reporting periods (RP) are:

- i. RP1: from month 1 to month 12
- ii. RP2: from month 13 to month 30
- iii. RP3: from month 31 to month 42

During the periodic reports, the following documents will be provided:

• Technical report: it contains the information about the progress of project activities per each WP and specific tasks complemented by the resources allocation and use during the period with a narrative description of the financial expenditures of the whole Consortium in terms of budget and person-months spent: assessment of the expenditures status vs the plan budget as per Grant Agreement and identification and justification of potential deviation. The Coordinator will fill the statement based on an internal monitoring excel file shared with the partners, which will be described in the next paragraph.

The Project Periodic Technical Report will follow the templates provided by the EC for the Horizon Europe Programme.

• *Financial costs :* expenditures confirmed by every partner via the ECAS portal in terms of budget and person/months spent.

The project Coordinator will ask in due time all partners to provide their inputs for the abovementioned documents, namely 15 days after the end of the reporting period, with a deadline for the end of the month.

3.4.2 Internal Reports

As part of an internal monitoring activity, the Coordinator has prepared a comprehensive excel file to keep track of the project financials and verify that they are in line with the activities plan set out in the Grant Agreement. The file reports the amount of budget and effort in terms of person/month spent by each partner. It also includes the calculation of the cumulative amount of budget and person months spent by the Consortium as a whole. As mentioned in the previous paragraph, this Excel file will be used during the official reporting periods to gather the relevant financial information that is essential for the Coordinator to fill the *Financial cost statement*. Partners will be required to provide input concerning their actual expenditures in terms of budget (personnel, other costs) and in terms of person-months. The file includes two sheets per partner to include this specific information. This information will automatically feed into the general overview of the total amount of budget and person months spent. This will serve as the base to assess the expenditures status vs the planned budget as per Grant Agreement and identification and justification of potential deviation.



In addition to the official periodical reporting, the same file will be used to gather from the partners an update related to the spending of personnel effort in terms of person/months. This information will be gathered every six months. The project partners will be asked to fill only their organisation's sheet specifying the total effort per WP per internal reporting period (M1-M6; WP7-12; M13-M18; etc..)

This Excel document is stored in the project shared repository.

3.5 Payments

Payments are regulated according to the Grant Agreement (articles 7 and 22) and to the CA (article 7.2).

Payments to partners are the exclusive task of the Coordinator. In particular, the Coordinator will:

- notify the partners concerned, promptly of the date and composition of the amount transferred to their bank account, giving the relevant references
- perform diligently its tasks in the proper administration of any funds and in maintaining financial accounts
- undertake to keep the Granting Authority's financial contribution to the Project separated from its normal business accounts, its own assets and property.

The transfer of the initial pre-financing, the additional pre-financings (if any) and interim payments to project partners will be handled in accordance with Article 22.1. and Article 7 of the Grant Agreement following this payment schedule:

- Funding of costs included in the Consortium Plan will be paid by the Coordinator to the project partners after receipt of payments from the Granting Authority without undue delay and in conformity with the provisions of the Grant Agreement. Costs accepted by the Granting Authority will be paid to the Party concerned.
- The Coordinator is entitled to withhold any payments due to a project partner identified by the General Assembly to be in breach of its obligations under this Consortium Agreement or the Grant Agreement or to a Beneficiary which has not yet signed the Consortium Agreement.
- The Coordinator is entitled to recover any payments already paid to a Defaulting project partner except the costs already claimed by the Defaulting partner and accepted by the Granting Authority. The Coordinator is equally entitled to withhold payments to a project partner when this is suggested by or agreed with the Granting Authority.

4 Quality Assurance Process

In this section, the main processes and strategies set out within the SYNERGIES project to ensure the quality of project activities and results are presented, describing in a pragmatic way the tools envisioned for such goal.

The SYNERGIES quality policy touches upon all the activities and results carried out within the project. Specific procedures have been established to ensure that the main instability sources (conflicts, change and deviations and other risks) are properly monitored, assessed and mitigated. Moreover, quality assurance impacts the production of project-related contents (documents, deliverables...). Therefore, precise processes have been established to ensure that the output respects the quality standards, starting from the naming and archiving of the file, the review and submission processes.

4.1 Quality Policy and principles

The main goal of project management is to provide a lean but effective framework to support the consortium in achieving the scientific, technical and business objectives of the project. Efficient decision-making processes and swift responsiveness to changing circumstances are required.

Quality assurance will be applied to all procedures and outputs (deliverables, documents) of the project. The Project Coordinator, with the support of the Technical Coordinator and the WP leaders, is responsible for the necessary assessment of deliverables.

The whole project consortium will be deeply committed to assuring high quality results and, for that reason, quality assurance will be the joint responsibility of all project partners at all levels. In this context, SYNERGIES has envisioned strategies such as conflict resolution and change management, as well as more practical measures such as standardised procedures for deliverable preparation, revision and submission. This provides all the partners with a solid and efficient framework, as well as a specific set of tools, that will allow them to produce project results that are in line with the expected quality level.

Moreover, a key aspect within the quality management is the project's risk management process, which is described more in detail in section 5 in terms of methodology and strategy to manage and contain risks. A continuous risk assessment will allow that, in case of problems, the required corrective actions are initiated in co-operation with the partners concerned, thus further ensuring the achievement of high-quality project results.

4.2 Conflict resolution

A sound procedure for conflict resolution among partners is indeed key to avoid a drop in the quality of project activities. Section 11.8 of the SYNERGIES Consortium Agreement describes the project rules on conflict resolution, which prescribe as follows:

The project partners will endeavor to settle their disputes amicably. Any dispute, controversy or claim arising under, out of or relating to this contract and any subsequent amendments of this contract, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, will be submitted to mediation in accordance with the World Intellectual Property Organization (WIPO) Mediation Rules. The place of mediation shall be Brussels unless otherwise agreed upon. The language to be used in the mediation shall be English unless otherwise agreed upon.

If, and to the extent that, any such dispute, controversy or claim has not been settled pursuant to the mediation within 60 calendar days of the commencement of the mediation, it shall, upon the filing of a Request for Arbitration by either project partner, be referred to and finally determined by arbitration in accordance with the WIPO Expedited Arbitration Rules. Alternatively, if, before the expiration of the said period of 60 calendar days, either project partner fails to participate or to continue to participate in the mediation, the dispute, controversy or claim shall, upon the filing of a Request for Arbitration by the other project partner, be referred to and finally determined by arbitration in

accordance with the WIPO Expedited Arbitration Rules. The place of arbitration shall be Brussels unless otherwise agreed upon. The language to be used in the arbitral proceedings shall be English unless otherwise agreed upon.

The award of the arbitration will be final and binding upon the Parties.

Nothing in this Consortium Agreement shall limit the Parties' right to seek injunctive relief in any applicable competent court.

In addition, specific provisions have been established to guarantee that any conflict that may arise during voting session of the main management bodies (General Assembly, Executive Board). The main instrument at the partners' disposal is the veto right. As set out in the CA, article 6.2.4, each partner has the right to veto decisions that

- are foreseen on the original meeting agenda
- affect severely that own work, time for performance, costs, liabilities, intellectual property rights or other legitimate interests.

When a decision has been taken without a meeting, a partner may veto such decision within 15 calendar days after written notice by the chairperson of the outcome of the vote.

In case of exercise of veto by a partner, the Members of the related Consortium Body shall make every effort to resolve the matter which occasioned the veto to the general satisfaction of all the partners.

Finally, given the SYNERGIES scope and solutions, special attention has been granted to potential emerging conflicts generated by access rights to software and licenses IPR. General principles for its resolution have been specified in section 9.8.2 of the CA, while the IPR management is fully described in section 8.

4.3 Change Management

Change management is envisioned as a key process of requesting, reviewing, approving, executing and monitoring changes to a project direction or core deliverables that will affect the project results, whether it is impact, budget, or timeframe, in view to an optimal flexibility and adjustment of the project activities towards the project goals. The SYNERGIES multi-level approach to change management is described below, including in detail the responsibilities and the tools to use in order to manage the change process.

Every SYNERGIES participant may raise a Request for Change (RFC). The Project Coordinator will then ensure that this is captured and proactively managed to conclusion. An initial review should be made to examine the need for the change, how it could be achieved and what the consequences might be. The most appropriate member of the Consortium will normally perform this review. Based on these conclusions, a recommended course of action will be proposed.

More specifically, the multi-level approach envisions six phases to go through any request for change:

- i. *Identification*: any SYNERGIES project partner may identify potential changes and record the issue.
- ii. *Validation*: the Project Coordinator collects the requests for change submitted and validates the request during a meeting with the project partners. The request is assesses based on its necessity to the project.
- iii. *Analysis*: the Project Coordinator, together with selected project partners, assesses the impact of the change on the project activities in terms of scope, schedule and budget.
- iv. *Decision*: if no impact is foreseen concerning the abovementioned dimensions, the Project Coordinator decides whether to approve or dismiss the request. The Project Coordinator can present and discuss the request with the General Assembly during the next meeting or an extra meeting, if urgent.



If the request for change is foreseen to impact on the project scope, schedule or budget, the project Coordinator will consult the Project Officer to come to a final decision concerning the request.

- Action: the Project Coordinator integrates the change into the project activities and submits ٧. the proposal to the PO, who will review and approve/dismiss/ask for a revision of the request.
- vi. Closure: The Project Coordinator closes the change request once the EC approval is received and communicates the result to the project partners.



Figure 3: SYNERGIES change management phases

As described in Article 39 of the Grant Agreement, if the request of change entails an official Amendment to the Grant Agreement, an official request should be sent through the Portal Amendment tool. Amendments can be requested by any of the project partners. The coordinator submits and receives requests for amendment on behalf of the project partners.

The request for amendment must include:

- the reasons why
- ٠ the appropriate supporting documents
- for a change of coordinator without its agreement: the opinion of the coordinator (or proof that this opinion has been requested in writing).

The Granting Authority may request additional information.

If the party receiving the request agrees, it must sign the amendment in the tool within 45 days of receiving notification (or any additional information the granting authority has requested). If it does not agree, it must formally notify its disagreement within the same deadline. The deadline may be extended, if necessary for the assessment of the request. If no notification is received within the deadline, the request is considered to have been rejected.

An amendment enters into force on the day of the signature of the receiving party.

An amendment takes effect on the date of entry into force or other date specified in the amendment.

4.4 Deliverable Preparation and Submission

Deliverables are the main outputs of SYNERGIES and are key to report to the EC the progress of the project, since they are the technical documents that contain the analysis of the results.

Therefore, a precise procedure for deliverable preparation, revision and submission is necessary to keep a consistent structure and presentation of the documents throughout the whole project lifetime and to ensure that the quality level meets the contractual obligations.

Each deliverable should be submitted to EC according to the schedule included in the DoA. Precise roles and responsibilities are assigned to project partners for the preparation and submission of such documents.

The detailed procedures will be described below.

4.4.1 File naming convention

A standard naming convention has been set by the Project Coordinator and shared with all the project partners to have a common methodology of how to store and search for deliverables and important documents in the shared repository. It allows a clear monitoring of any missing deliverables and it helps to identify older and revised versions of the same document. For the deliverables, the following naming convention has been agreed on:



PROJECT NAME_D- n. of the deliverable - name of the deliverable_v. (number of version)

Example: SYNERGIES_D1.1 Project Management Plan-v0.1

A similar methodology has been adopted for internal deliverables, which have been named as follows:

PROJECT NAME_ID(internal deliverable) - n. of the WP - .0+n (progressive n.)- internal deliverable name

Example: SYNERGIES ID 2.01 Draft MVP and Business and user requirements-v0.20

4.4.2 Deliverable Submission Process

The goal of the process is to assure the timely submission of the deliverable and the high quality of the document, in line with the contractual obligations in the DoA.

The main general rules that apply to the creation of Deliverables are:

- Deliverables must be finalized and submitted to the EC within the deadlines defined in Part A (DoA) of the Grant Agreement.
- ٠ Each deliverable is associated to a project partner which is fully responsible for the deliverable quality and timely submission, and for the coordination of the participants to get adequate contributions.
- The Deliverable template is available in the project shared repository.
- The submission to the EC is done by the Project Coordinator via the participant portal electronically.

Deliverables and Internal Deliverables will be submitted/finalized according to the deadlines shown in the table 2 and table 3 in section 3.1.

The submission of a deliverable is a process with several intermediate stages that must be completed before it reaches the submission phase. In terms of timing, the preparation and submission of a deliverable will follow the following procedure:

Timing before the delivery date	Action					
2 months	The partner responsible for the Deliverable sends the proposed Table of Contents (ToC) to the partners involved, distributing the responsibilities per section.					
1,5 month	The partners involved send their draft contributions to the ToC.					
20 days	The partners involved send back the final contributions for their sections.					
15 days	Preparation of first version of the Deliverable by the Partner responsible for the Deliverable, to be circulated to the peer internal reviewers.					
7 days	Integration of the feedback from the peer internal reviewers by the Partner responsible for the Deliverable and preparation of the pre-final draft.					
5 days	Confirmation by the peer-reviewers that the changes made (by the Deliverable authors) appropriately address their review feedback.					
3 days	Final version circulated by the Deliverable's responsible partner to the Project coordination for final review.					



Timing before the delivery date	Action				
Due date	The project coordinator submits the Deliverable to the EC and uploads the document to the shared repository.				
Table 1: SYNERGIES deliverable submission procedure					

Table 4: SYNERGIES deliverable submission procedure

In case any delays are expected, the Project Coordinator will promptly inform the Project Officer.

4.4.3 Deliverables Review process

As mentioned in section 3.1 of the present Deliverable, a set of two internal peer reviewers is associated to each Deliverable, in order to guarantee the high quality of the results and that the deliverables' contents are complete and consistent with the project's goals and scope. The peer review team will check their quality before the final submission to the EC by the Project Coordinator.

The general criteria for nominating reviewers are:

- The author(s) of the deliverable cannot be nominated as a reviewer of the deliverable. i.
- ii. The Work Package Leader or Task Leaders cannot be appointed as the reviewers of the deliverable that is related to the WP.
- iii. The internal reviewers are selected considering their total effort in the project, in order to allocate the workload equally among the partners. Moreover, internal deliverables are assigned to reviewers that, although not part of the specific WP, have somewhat experience in the activities reported in the internal deliverable.

The coordination team has elaborated a plan which defines the partners in charge of the internal review of the SYNERGIES deliverables, which can be found in the tables in section 3.1.1 (Official Deliverables) and 3.1.2 (Internal Deliverables).

The internal reviewing procedure is one of the main tools to guarantee the high quality of the results. Each WP leader will be responsible for the quality of the results, which will be subject to a peer review by the selected internal reviewers. The peer review team must check their quality before the final submission to the EC, providing their feedback using the "track change" mode. The last review of the Deliverables is carried out by the Project Coordinator, before finally submitting the Deliverable.

5 Risk Assesment

This section illustrates the overall process for the risk management of the SYNERGIES project and presents the results of the initial risk analysis conducted by the Consortium partners.

5.1 Scope

According to ISO 31000¹, a risk reflects the effect of uncertainty on objectives while, in alignment with the latest edition of the PMBOK Guide², a project risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives, such as scope, schedule, cost or quality. Risk Management is generally the process of identifying, assessing, responding to, monitoring, and reporting risks and, when performed successfully, provides several benefits, e.g.: improving product quality, enabling better use of resources, preventing problems before they occur, and proactively identifying and addressing potential issues.

In this context, applying an effective and iterative method to continuously manage and monitor risks is considered as instrumental for the successful implementation of the SYNERGIES project. In SYNERGIES, the Risk Management Plan defines how risks associated with the project will be timely identified, analysed, and managed to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. It outlines how risk management activities will be performed, recorded, and monitored in a systematic manner throughout the lifecycle of the project, while providing templates and practices for recording and prioritizing risks, foreseeing the consequences and effectively managing them through appropriate proactive actions.

With the purpose of assuring that risk-related uncertainty does not deflect the SYNERGIES project from its objectives as stated in its Description of Action, the present Risk Management Plan is created by the Risk & Quality Manager with the help of the Project Coordinator, the Technical Coordinator and all Work Package leaders and shall be continuously monitored and updated throughout the project.

The intended audience of this plan involves the whole project management and implementation team, as risk awareness amongst all partners of the SYNERGIES Consortium constitutes an important additional risk management factor.

5.2 Continuous Risk Management Methodology

The SYNERGIES risk management methodology has been designed on the basis of existing risk management practices and standards, including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards. In particular, the project risk management approach proposed in the PMBOK guide and the Continuous Risk Management approach developed by the Software Engineering Institute (SEI) of Carnegie Mellon University³ are mainly leveraged as proven software engineering practices with processes, methods, and tools for managing risks in ambitious projects like SYNERGIES.

¹ ISO 31000 – Risk management. Online: <u>https://www.iso.org/iso-31000-risk-management.html</u>

² A Guide to the Project Management Body of Knowledge (PMBOK[®] Guide). Online: <u>https://www.pmi.org/pmbok-guide-standards/foundational/pmbok</u>

³ Audrey J. Dorofee, Julie A. Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy and Ray C. Williams, Continuous Risk Management Guidebook, Software Engineering Institute of Carnegie Melon University. Online: <u>http://jodypaul.com/SWE/ContinuousRiskManagement.pdf</u>


Figure 4: Continuous Risk Management in SYNERGIES.

As depicted in Figure 4 the risk management approach adopted and iteratively applied in SYNERGIES bears four phases, including:

- 1. **Risk Identification phase**, that determines which risks are likely to affect the project and extracts their characteristics in a structured manner through internal brainstorming at project / work package level.
- II. Qualitative Risk Analysis phase aiming at evaluating risks and risk interactions to assess the range of possible project outcomes and the project activities' vulnerability to specific risks. During this phase, the risks are assessed, correlated and prioritized on the basis of experts' judgments (namely of the WP Leaders) with the help of the impact/likelihood model that SYNERGIES has adopted. Such a model features two risk assessment dimensions, as follows:
 - <u>Likelihood</u>, representing the possibility or potential frequency that a considered risk (or unexpected event) may occur. Likelihood is expressed using qualitative terms, e.g.:
 - Low: the risk is not likely to occur (<30% chance) during the project lifetime.
 - *Medium*: the risk is relatively likely to occur (30% up to 70% chance) during the project lifetime.
 - *High*: the risk is very *likely* to occur (>70% chance) during the project lifetime.
 - <u>Impact</u>, related to the effect of the risk occurrence on the project (e.g. on its results, performance, cost, or time plan) and measured in 3 scales:
 - *High*: the effect will strongly disturb the project, and the effort or lead-time to recover will be *significant* or even too long to reach expected objectives on time.
 - *Medium*: the effect will disturb the project, but will not impact the duration of the project or *attainment* of objectives.
 - *Low*: the effect will slightly disturb the project, but the project can rapidly recover and return on track.
 - <u>Risk Exposure</u> is a risk indicator created by combining the impact and likelihood of the risk. The following <u>table</u> defines the severity of risks resulting from the impact/likelihood model.

Risk Exposure		Risk Impact		
		Low	Medium	High
Diale	Low	Low	Low	Medium
Likelihood	Medium	Low	Medium	High
	High	Medium	High	High

Table 5: Risk exposure definition table.

- III. Risk Response Planning phase, that defines responses to threats and enhancement steps for opportunities. In SYNERGIES, responses to threats are generally oriented towards mitigation. During this phase, the Risk Symptoms / Triggering Factors for Action are described in detail, in order to allow the risk owners to early identify indirect manifestations of actual risk events. In addition, Risk Control & Mitigation Actions are defined (especially for risks where exposure is high) to reduce the chance of risk materialization and/or impact (*ex-ante*).
- IV. Risk Monitoring & Control phase to execute the risk management plan and timely respond to risk events over the course of the project. This phase involves continuously tracking and assessing identified risks, early identifying symptoms for risks that have been ranked as with high and medium exposure, and timely responding to changes in risks' status / exposure over the course of the SYNERGIES project implementation. To this direction, concrete Risk Contingency / Recovery Actions are already identified and shall be triggered if a risk actually occurs (*ex-post*).

In SYNERGIES, a risk information template has been created (see Table below) and shall be used for identifying new risks, as well as for modifying the status of risks, tracking the status and monitoring the mitigation strategy evolution. Work Package Leaders are responsible for complementing the template for risks related to their respective work packages. The different management, technical and impact risks are consolidated by the Risk & Quality Manager, who maintains an updated version of the Risk Management Plan for the project.

#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
MNGM-i		{r M H}	{r M H}	{r M H}					
TECH-j		{H W H}	{H W H}	{H M H}					
IMP-k		{r M H}	{r M H}	{r M H}					

Table 6: Risk Definition template.



Risk Registry and Contingency Plan 5.3

At the very beginning of the SYNERGIES project, a set of risks associated to the work that will be undertaken in each work package at technical, business and management level has been identified with the collaboration of all WP Leaders, complementing the list of risks that have been already identified in the SYNERGIES DoA.

The following table presents the lists of risks the project has identified, assessed and managed on M3 of the SYNERGIES project implementation. Such an initial list of risks is bound to evolve over time due to the developments of the project and its achievements, and includes the risks re-evaluation in terms of impact and likelihood. To this end, the role of the Risk Monitoring & Control phase as well as of the iteration of all risk management phases defined in Figure 44 is very crucial.

#		Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
MN -1	GΜ	Losing critical staff or partners at crucial point of the project	L	Н	М	 Very poor involvement and/or significant lack of interest in the project activities of a specific partner. Partner identified as "Defaulting Party" as per the rules stated in the Consortium Agreement. 	 Continuous quality control activity to early discover any potential performance issue. At least 2 contact points to be appointed per partner to follow the project activities Keep close contact with all partners to early identify any serious problems 	 Project Coordinator to immediately inform the Project Officer to explain the reasons of a partner withdrawal and to propose a solution Enough diversity and expertise to address losses within organizations or the consortium Immediate take-over of the leaving partner's tasks and responsibilities by other partner(s) or by other team members 	• M1- M42	• TXT, ALL



#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
MGMT- 2	Delays in key milestones or critical deliverables	Μ	Н	Н	 Missing the internal deadlines set for the official project deliverables. Delays in the work towards key milestones. 	 Definition of a reference timetable for internal deliverables to ensure the release of the deliverables on time. Continuous monitoring of the progress by the WP leaders, the Project Coordinator, and the Technical Coordinator, sending reminders to partners through regular communication by email and during the physical/virtual meetings. 	 Proposal of a corrective time plan by the lead partner to deal with the consequences of the delay. Agreement among all involved / affected partners. Project Coordinator to immediately inform the Project Officer to the cause of the delay and the contingency plan. Note: If a deadline has been missed exclusively due to the negligence of a partner, the Project Coordinator will give formal notice to such partner requiring corrective actions. 	M1- M42	TXT, ALL
MGMT- 3	Insufficient quality of results	L	Н	М	 Numerous and serious negative evaluations during the internal peer review process. Negative outcomes from the EC periodic reviews. Extremely poor interest expressed about the project activities. 	 Consortium synthesis bringing together experienced partners dedicated to contributing, each in their respective area of expertise, to the successful implementation of the project objectives. Risk & Quality Manager role foreseen in the SYNERGIES Project Management structure to oversee the quality assurance procedures and guarantee the expected quality of the works along the project lifetime with the support of the Project and Technical Coordinators. 	 The Project and Technical Coordinators to identify and propose corrective actions to improve the quality of the work within the timeframe set. Note: If the insufficient quality of the results is exclusively due to the negligence of a partner, the Project Coordinator will give formal notice to such partner requiring corrective actions. 	M1- M42	Suite5 <i>,</i> TXT, ALL



#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
MGMT- 4	Lack of communication and/or alignment among the consortium partners	Μ	Σ	×	 Low usage of the project collaboration tools (mailing- lists, private area of the project website, teleconferencing tool,). Poor participation in the teleconferences and/or in the project meetings. Work not aligned within and across WPs as expected. Continuous disagreements between partners. 	 Close contact with all partners through regular teleconferences and virtual meetings. Organize regular plenary and technical meetings at different partners' sites. Provide guidance for the use of online collaboration tools. 	 Organization of extra meetings, at WP, Task or consortium level, online and/or face to face. Reinforce/reconsider the use of the selected communication/collaboration tools. Detailed project plan that clearly states goals and responsibilities of the partners. Project and Technical Coordinators to discuss and resolve any conflicts. If necessary, the consortium will decide the solution according to the CA. 	M1- M42	TXT, ALL
MGMT- 5	Overspending of resources and/or allocated budget	L	L	L	 Average expected spending of resources (effort and/or budget) exceeded in the internal administrative/financial reports. 	 Keep close contact with all partners to early identify possible overspending. Periodic administrative reports carried out to check the status of the project expenses (in terms of both effort and budget). 	 Verify the possibility of a budget and workplan revision to redistribute tasks, effort and funding among the Consortium. Make binding agreements on the finalization of the planned works, regardless of any overspending conditions. 	M1- M42	TXT, ALL



#	:	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
N 6	ИGMT-	Ethics requirements not correctly / sufficiently handled	L	Н	L	Effective compliance with the General Data Protection Regulation.	Put emphasis on management of personal data at an early project stage, also, through the appropriate documentation of the related data sets, for instance, under the D1.2 on Data Management Plan. Raise awareness within the consortium regarding the necessity by relevant partners to conduct a Data Protection Impact Assessment periodically, also, due to the use of Artificial Intelligence. Provide information to the participants in the engagement activities in a clear language, e.g. providing for information in an understandable language for non-experts.	Consideration of the findings of the periodical Data Protection Impact Assessments and implementation of revised technical and organizational measures, if necessary. Ad hoc support to technical partners handling personal data through dedicated meetings.	M1- M42	ALBV



#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
TECH-1	Performed design is ineffective resulting in project drifting into wrong direction	L	н	м	 Difficulty in reaching consensus on the use cases, requirements and architecture. Difficulty in mapping the architectural components to latest technological developments, underlying trends and state-of-the art platforms. 	 Experience and knowledge of the domains involved and coupled in SYNERGIES brought by the Technical Coordinator and technical partners, holding similar roles in relevant previous and on- going R&I activities Technical Coordinator to monitor the design process to quickly identify ineffective designs and take proactive measures. State-of-play analysis and technology watch continuously performed over the course of the specifications elicitation. Constant monitoring of trends related to Energy Data Spaces. Collaboration with other Energy Data Spaces Projects 	• Adapt/redesign the use cases / requirements / reference architecture to incorporate the necessary latest developments.	M1- M28	ICCS, Suite5, TXT, ALL



#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
TECH-2	Significant deviations from the planned technical expectations	L	Н	М	 Delays in the delivery of critical functionalities Misalignment in the design and/or integration of components 	 Early detection of deviations through agile development, periodically verified in all project meetings and through online collaboration tools Definition of the MVP to prioritise functionalities and bring all partners on the same page. Integration of mature technologies minimizing the chance of significant deviations Technical coordinator to continuously monitor the technical development process 	 Technical Coordinator to adapt the development and integration plan in collaboration with the technical WPs, moving effort to implement the required functionalities Organization of technical-business users sessions, training webinars and demo sessions. 	M1- M42	Suite5, TXT, ALL
TECH-3	Lack of maturity of key technological components / solutions	L	Н	М	 Performance issues or misbehaviour in comparison to the requirements Low quality of the source code Delays in the software delivery based on the development plan Technology replacement cases 	 Verification of technologies in periodic technical meetings All technologies to be used as reference for the implementation (technology brought from partners) to be already in - at least - TRL 4 to 5 Continuous monitoring of the development progress through stand-up meetings and demos Continuous assessment of the software quality and quality assurance. Code coverage metrics defined since the beginning of the development activities 	 Technical Coordinator to identify any software components/solutions that are lagging behind and agree on a strict contingency plan with all involved partners. Allocation of the appropriate effort for providing refactored/improved/new solutions on time. 	M6- M36	Suite5, Technical Partners



#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
TECH-4	Interoperability problems between components that have been built on heterogeneous frameworks	м	м	М	 Incompatible interfaces between components that need to interact and exchange information. Delays in the completion of intermediate milestones in the integration plan 	 Use of best practices to prevent interoperability thrust while assessing the design specifications for each component. Compliance with available open standards for standards-based interoperability. Continuous integration and continuous delivery processes and tools in place. Consortium partners' deep knowledge of interoperability issues to be addressed in the project Technical partners to agree on issues that may impact interoperability from the design phase. 	 Technical Coordinator to convene appropriate meetings to agree on the best solution for integrating the problematic components Allocation of the appropriate effort for reworking/adapting the needed interfaces, designing new APIs or developing an alternative solution in the time frame set 	M6- M36	Suite5, Technical Partners



#		Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
Т	ECH-5	Problems due to the strong reliance on previous projects' results (H2O2O- SYNERGY) for the delivery of the SYNERGIES Energy Data Space	L	Н	м	 Delays in the delivery of the final release of the H2020- SYNERGY Platform (expected in December 2022) Critical functionalities considered as available for SYNERGIES, eventually missing from the H2020-SYNERGY Platform 	 Careful alignment between the end of the development activities of the H2020-SYNERGY Project and the start of the development activities of the SYNERGIES Project. Quality of H2020-SYNERGY results already validated by the H2020-SYNERGY project partners (in the 1st demo run), the EC and reviewers in 2 review meetings. Technical partners involved in the H2020-SYNERGY Platform development (Suite5-Technical Coordinator in both projects, Ubitech, Maggioli, ETRA), also involved in the SYNERGIES project and fully committed in further advancing and extending its components and services. Technical Coordinator (Suite5), being also the Technical Coordinator in H2020-SYNERGY, to supervise and coordinate the development process to ensure the smooth transition 	 Technical coordinator to identify changes in the SYNERGIES reference architecture and define a revised development plan Technical partners to propose alternative solutions for any component that is not eventually adopted from H2020-SYNERGY 	M1-M4	Suite5, Technical Partners



#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
TECH-6	Reluctance from demo partners to provide data due to confidentiality and security issues.	Μ	Н	Н	 Delays in providing the necessary info for the in-depth profiling of the available data assets and energy assets (infrastructure) Slow/limited progress in the availability of the demo data (at the expected volume, velocity and granularity) to the SYNERGIES Energy Data Space 	 Consortium Agreement will define the terms regarding access to data and existing knowledge Secure mechanisms will be deployed for data sovereignty and sharing for data which is characterized as "sensitive" and "confidential" Continuous engagement activities for removing relevant barriers through the SYNERGIES Living Labs 	 Demo partners to present a concrete plan for making available alternative, real data assets of equivalent volumes, velocity, granularity and overall features Project and Technical Coordinator, WP5 Leader, to agree with the affected demo partner on the contingency measures 	M1- M42	Demo Partners, ALL
IMP-1	Limited access to demo sites and delay in gathering demo information and implementing project demo actions.	м	Н	н	 Delays in meeting the intermediate milestones set Delays in the installation of required equipment. Slow/limited progress in the availability of the demo data (at the expected volume, velocity and granularity) to the SYNERGIES Energy Data Space. 	 Proactive measures with the demo partners to accelerate information collection and procurement processes to create a buffer of time that can be utilized in case of restrictions Technical team always alert to speed up deployment 	 Demo partners to initiate discussions for alternative demo locations and legitimate actions (e.g., special permits) to be undertaken to ensure the realization of the demo activities Project and Technical Coordinator, WP5 Leader, WP5 Task Leaders to agree with the affected demo partner on the contingency measures 	M12- M42	Demo Partners, ALL



#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
IMP-2	Limited acceptance by the end-users	L	н	м	 Limited feedback gathered for demonstrators' evaluation Limited interactions by end users initiated for support High learning curve for end- users due to high level of expertise required 	 Continuous engagement through the user-centric approach brought by the SYNERGIES Living Labs, allowing end-users (within and beyond the SYNERGIES consortium) to get engaged and provide feedback across all phases of project implementation Early prototyping of simple mock-ups (non-functional) to assess usability. Iterative validation process for the demo partners to raise awareness of relevant developments, participate in dedicated demonstrations of the SYNERGIES results prior to their intermediate and final releases and provide early feedback for improvements and adaptations 	 Organization of technical-business users' sessions, training webinars and demo sessions to ensure co-creation with the end-users towards enhanced acceptance. Cost-benefit assessment of the SYNERGIES results to ensure that the end users realize in full breadth the significant benefits realized across the value chain both in economic, societal and environmental levels 	M12- M42	PI, TXT, Suite5, ALL



#	Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
IMP-3	Out of the radar competition hindering the exploitation of results	м	Σ	м	 Projects results not aligned with the current market trends at any time during the project lifetime. Low interest in the project results by the targeted stakeholders 	 Market intelligence activities, as part of the exploitation planning, to ensure continuous monitoring of the competition landscape. Close interaction with sister projects (as part of WP7) activities, to reveal critical success factors and features that need to be included in the SYNERGIES offering, while alerting the consortium for the acceleration of the planned developments and associated exploitation activities to effectively and timely reach the market with a highly competitive solution in the Energy Data Spaces arena, against competition WP6 and WP7 Leaders to ensure the thoroughness and quality of the relevant activities and resulting reports 	• WP6 and WP7 leaders to initiate discussions with the technical WPs to assess if design changes are feasible so as to competitively align results with market trends	M1- M42	TXT, ALL



#		Risk Description	Likelihood	Impact	Exposure	Risk Symptoms / Triggering Factors for Action	Risk Control & Mitigation Actions (to reduce probability and/or impact)	Risk Contingency / Recovery Actions (if the risk actually occurs)	Risk Validity Period	Risk Owners
IMF	P-4	Disputes over ownership of IPR amongst consortium partners	М	L	L	 Disagreements in the consortium over ownership results, e.g., when applying licenses to software components released from SYNERGIES. Individual partners business exploitation plans are not aligned with the expected assets outcoming from SYNERGIES. 	 Standard IPR and access rights clauses included in the CA which was signed before the project starts. Continuous IPR handling. Creation of an ongoing IPR inventory. 	 Project Coordinator to organize meetings to discuss and resolve any conflicts. Apply the principles included in the Consortium Agreement and the Grant Agreement. Further support to be provided by the legal experts involved in the project for IP conflict resolution 	M1- M42	TXT, ALL
IMF	P-5	Limited effectiveness of dissemination and engagement due to COVID restrictions	н	Н	Н	 Contributions to the activities defined in WP6 are misaligned or not as well received as it was expected. Underperformance in key dissemination and engagement KPIs 	• Employment of alternative methods for stakeholder engagement and dissemination (Online workshops/interviews, virtual events, etc.) with which the majority of people have familiarized during the last 2 years and have gained in effectiveness	 Revisit communication and dissemination plans to reinforce any well-performing activities and/or adopt additional dissemination/engagement channels 	M1- M42	TXT, ALL

Table 7: List of risks identified by SYNERGIES

SYNERGIES Shaping consumer-inclusive data pathwaYs towards the eNERGy transItion, through a reference Energy data Space implementation

6 Ethics approach

6.1 Ethical Aspects of Data and Artificial Intelligence

This section outlines certain ethical principles to guide the partners of the SYNERGIES project, in view of deciding upon purely technical matters and further proceeding with their implementation. Having taken into account that SYNERGIES envisions the use of data to create an Energy Data Space and deploying Artificial Intelligence (AI) systems to provide data-driven services, these principles are of horizontal relevance for all the activities envisioned to be undertaken by the project. Therefore, giving rise to two main ethical considerations, namely, data ethics and AI ethics. The following sections will outline the framework for these ethical principles and subsequently, provide an overview of which elements of the SYNERGIES project assists in achieving these aims.

6.1.1 Data Ethics

There is much to be gained from sharing data. However, care must be taken to ensure that data sharing is conducted in accordance with the principles of ethical data sharing. Therefore, approaching data sharing ethically is a balancing exercise. The SYNERGIES project aims to collect prosumer-related data using smart meters and sensors to create context-aware flexibility profiles.

The collection and subsequent analysis of large datasets may give rise to various ethical issues. These ethical issues include, among others, the misuse of data, data-driven discrimination and bias. The challenge is to enable the sharing of data while ensuring that individuals are able and empowered to enjoy and exercise their fundamental rights. Data sharing and access to data require the creation of a trusted environment with sufficient levels of transparency and compliance with the regulatory framework on data protection.

How can this trusted environment be created, and how can data sharing adhere to these overarching ethical principles? SYNERGIES involves the collection of prosumer-related data, which will include among others, personal data. Therefore, it is crucial to ensure that individuals involved are placed at the centre of the innovative initiative by enabling individual control, transparency, accountability, and equality in how data is utilised within the project.

Individual Control and Data Ownership

In deploying data-driven technologies, particularly those that collect and share personal data. It is crucial that individuals retain control of their personal data. Adhering to one of the key principles set out in the European Union's Declaration on Digital Rights, namely putting people at the centre; enabling individual control represents, is a central element to this notion.

Freely given, specific and informed consent, as set forth in the General Data Protection Regulation (GDPR),⁴ is a legal construct that supports the concept of data control. However, it is not sufficient to simply ensure that participants of the SYNERGIES project simply check a consent box without truly understanding what personal data will be collected and how those personal data are processed during the course of the project. In order to facilitate understanding, it is vital to ensure that communication regarding the data processing activities of the SYNERGIES project is clear and accessible to all the individuals whose data will be collected. Particularly, due to the use of sensors and smart meters within the project, it is not always obvious when and why personal data is being collected and how it is subsequently processed.

The importance of informed consent as an ethical principle and its existence in regulatory frameworks does not entail that opting in is the only option. To ensure that individuals remain in control of their personal data, technical measures must be taken to guarantee that individuals are also able to opt-

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation) OJ L 119, available at: <u>https://eur-lex.europa.eu/eli/reg/2016/679/oj.</u>



out of the collection of personal data, at any time in the course of the project. Moreover, technical measures must also be put in place to facilitate that individuals have the right to access, port, or erase their data if they so wish. Importantly, it must be clearly communicated to the individuals how to exercise these rights.

The SYNERGIES project seeks to prioritize consumers and introduce them as data owners and providers. Therefore, it must be appropriately communicated to consumers what ownership of the data entails within the scope of the project.

Transparency

In addition to transparency being a guiding principle to ensure that individuals are offered the appropriate level of control with regard to their data, the notion of transparency is also crucial in other facets of the SYNERGIES project. The project seeks to implement an Energy Data Space consisting of data from diverse energy actors. Therefore, it is necessary to ensure that there are appropriate levels of transparency are achieved in reference to the types of data used to drive innovation and determine the sharing potential across the energy data value chain.

With reference to the consumer, there must also be appropriate transparency on how the flexibility capacity of consumers is determined and what data is utilised to maximise self-consumption on the community and building level. Moreover, transparency on the data streams utilised to deliver personalised services and automated features must be provided to consumers.

Accountability

Accountability represents a key ethical principle; it entails that someone can be held responsible for their actions. The notion of accountability represents a slightly stricter form of responsibility. In the data exchange market, the issue of accountability is a rather complex one. Within the SYNERGIES project, there must be appropriate accountability mechanisms to ensure that consumers participating in the project can effectively hold someone accountable when things go wrong. For example, who can be held accountable should the personal data of consumers fall into the wrong hands or are misused?

Consumers need to have the ability to hold someone accountable for any harm caused and, where appropriate, must be able to ensure they can receive compensation for any damages suffered. The notion of accountability is about owning and co-owning roles and responsibilities, making things happen, and offering assistance should anything go wrong. Therefore, accountability must not be an afterthought but should be engrained throughout the various technical measures of the project and appropriately communicated to consumers.

To ensure accountability, mechanisms that facilitate the system's auditability must be established. For example, ensuring traceability and logging of the AI system's processes and outcomes. Risk and impact assessments must be conducted which takes into account various stakeholders that are (in)directly affected. Training and education must be provided to help develop accountability practices.⁵

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

A thorough and holistic risk mapping approach allows for selecting the right principles and giving each principle appropriate weight in comparison to the others. In the context of SYNERGIES, risks could, for example, arise from the exchange of data between connected devices. The constant interactions between devices make the system more vulnerable to potential risk. It is therefore required to build

⁵ European Commission, Directorate-General for Communications Networks, Content and Technology, Ethics guidelines for trustworthy AI, Publications Office, 2019, https://data.europa.eu/doi/10.2759/346720.



in trust, privacy protection and security mechanisms, among others. Without taking care of the risks and mitigating them with these principles, the technological systems – devices, networks, algorithms - will eventually fail, possibly leading to unintended consequences.

Data-driven discrimination and data bias

The principle of non-discrimination is encoded in the Charter of Fundamental Rights of the European Union.⁶ This principle prohibits "any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, languages, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation."

In order to get algorithms to run, data is required. These data are the drivers of the decision-making processes; however, data can be inaccurate, incomplete, outdated or even include certain biases. As a result, discriminatory outcomes for specific individuals or groups of individuals further exacerbating discrimination that already exists in the real world. Particularly, when data is processed through algorithmic systems, it is difficult to understand how decisions are made. Therefore, it is crucial that there is sufficient forethought placed in data selection and provenance.

Transparency on how algorithms are built and deployed is crucial. Moreover, conducting fundamental rights impact assessments, which include, among others, an assessment of the potential for discrimination in relation to different grounds. There must be the appropriate technical and procedural mechanisms in place to check the quality of the data.

6.1.2 Artificial Intelligence Ethics

SYNERGIES aims at providing ML-enabled data analytics and Digital Twin-based management services in an online platform. This entails that machine learning / deep learning models and various analytics techniques will be tested and implemented within the project. On this basis it seems appropriate to devote a section on the ethics of artificial intelligence. Thus, this section first examines if the tools developed by the consortium are likely to fall under the definition of artificial intelligence and, second, provides an overview of the guiding ethical principle and standards concerning AI.

Definition of Artificial Intelligence

There is no universally accepted binding artificial intelligence definition. In fact, almost all the proposed definitions of AI are still controversial and currently under debate. However, very recently, a definition of AI is provided by the high-level expert group on artificial intelligence assembled by the European Commission (AI HLEG) in the Ethics Guidelines for Trustworthy AI. Accordingly, AI systems are defined as software and/or hardware systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge or processing the information, derived from the data and deciding the best action(s) to achieve a given goal. Al systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how their environment is affected by their previous actions [...]"⁷. Later on, building on this definition, the European Commission provided a relatively narrower legal definition in the proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (hereinafter referred as "AI Act")⁸. According to Article 3(1) of the AI Act, an AI system means software that is developed with machine learning approaches, logic-and knowledge-based approaches or statistical approaches including Bayesian estimation, search and optimization method and can, for a given set

⁶ European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

⁷ High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019. Available at <u>https://digital-</u> strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

⁸ European Commission, proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts, COM/2021/206, available at https://eurlex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. Considering the anticipated impact of the AI Act across the Union, SYNERGIES adopts this legal definition for the ethics assessment practices.

Trustworthy Artificial Intelligence

Trustworthiness is a prerequisite for individuals and societies to develop, deploy and use AI systems. Without AI systems and the human beings behind them being demonstrably worthy of trust, unwanted consequences may ensue, and their uptake might be hindered, preventing the realisation of the potentially vast social and economic benefits that they can bring. To help Europe realise those benefits, it is important to ensure and scale trustworthy AI. Trust in the development, deployment and use of AI systems includes not only the technology's inherent properties, but also the qualities of the socio-technical systems involving AI applications. Hence, trustworthy AI concerns not only the trustworthiness of the AI system itself, but requires a holistic and systemic approach, encompassing the trustworthiness of all actors and processes that are part of the system's socio-technical context throughout its entire life cycle.

The AI HLEG Guidelines describe the need for trustworthy AI systems to be human-centric, to serve humanity and with the goal to improve human welfare and freedom.⁹ This approach entails maximising the positive outcomes of AI systems and minimising their risks in order to prevent harm. Building on human centricity, the AI HLEG determine the need for an ethical AI as one of the three main components necessary to build trustworthy AI. Accordingly, a trustworthy AI has three components, which should be met throughout the system's entire life cycle:

- AI should be <u>lawful</u>, complying with all applicable laws;
- AI should be <u>ethical</u>, ensuring adherence to ethical principles and values; and
- Al should be <u>robust</u>, both from a technical and social perspective, since, even with good intentions.

Ethics is the core pillar and it complements other two pillars. The ethics does not only aim at enhancing the protection bestowed on the individual rights like freedom and privacy, equality and fairness, but also avoiding harm, promoting individual and environmental well-being, and building a better and more sustainable society. Therefore, the following section briefly explain guiding ethical principle to which the designer and operators of AI systems should adhere in order to deploy a trustworthy AI.

Ethical Principles for Trustworthy Artificial Intelligence

Although the rapid increase in AI applications has led public-sector organisations and the competent regulatory authorities across the Union to issue principles, guidelines, and other soft law instruments for the ethical use of AI, this section analyses ethical principles set out under two prominent and perhaps, most influential documents for the project, i.e., the European Commission's Guidelines on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence¹⁰ which is developed from the HLEG's Ethics Guidelines for Trustworthy AI and the Recommendation of the Council on Artificial Intelligence by the OECD.11 Because all these instruments on "ethical AI" seem to overlap in a set of generic principles that could enable the development of ethical AI. Therefore, the SYNERGIES consortium considers the following six (6) high level principles of the ethical AI determined under these documents.

⁹ High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019, p4.

¹⁰ European Commission, Ethics by Design and Ethics of Use Approaches for Artificial Intelligence, Version 1.0, November 2021.

¹¹ Organisation for Economic Co-operation and Development, Recommendation Of The Council On Artificial Intelligence, LEGAL/0449, 22 May 2019. Available at <u>https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#dates</u>.



Respect for human autonomy. In practice, the principle of respect for human autonomy means that humans interacting with AI systems must be able to keep full and effective self-determination and to partake in the democratic process. It encapsulates three more specific principles, which define fundamental human rights: autonomy, dignity and freedom. AI systems should not unjustifiably subordinate, coerce, deceive, manipulate, condition or herd humans. Instead, they should be designed to augment, complement and empower human cognitive, social and cultural skills. The allocation of functions between humans and AI systems should follow human-centric design principles and leave meaningful opportunity for human choice.

Privacy & Data Governance. Al systems must guarantee privacy and data protection throughout a system's entire lifecycle. Therefore, AI systems must be built in a way that embeds the principles of data minimisation and data protection by design and by default as prescribed by the GDPR. This covers both the information provided by the user, and the information generated about the user over the course of their interaction with the system (e.g. outputs that the AI system generated for specific users or how users responded to particular recommendations). It must also be ensured users' data will not be used to discriminate against them unlawfully or unfairly. Quality and integrity of data must be ensured through appropriate data governance models that ensure data accuracy and representativeness and enable humans to actively manage their personal data and the way the system uses it.

Fairness. It implies a commitment to ensuring equal and just distribution of both benefits and costs and ensuring that individuals and groups are free from unfair bias, discrimination and stigmatisation. Moreover, the use of AI systems should never lead to people being deceived or unjustifiably impaired in their freedom of choice. Fairness implies that AI practitioners should respect the principle of proportionality between means and ends and consider carefully how to balance competing interests and objectives. The procedural dimension of fairness also entails the ability to contest and seek effective redress against decisions made by AI systems. Substantive fairness entails that the AI does not foster discrimination patterns that unduly burden individuals and/or groups for their specific vulnerability.

Prevention of harm, safety and well-being. The prevention of harm principle means that AI systems and the environments in which they operate must be safe and secure. This entails the protection of human dignity as well as mental and physical integrity. They must be technically robust and should not cause or exacerbate adverse impacts due to asymmetries of power or information, such as between businesses and consumers or governments and citizens. Preventing harm also entails consideration of the natural environment and all living beings. Al systems should also strive to make a positive contribution to these forms of well-being. To realize this goal, possible research participants, end-users, affected individual and communities and relevant stakeholders should be identified at the very early stage, to allow for a realistic assessment of how the AI system could enhance or harm their well-being

Transparency and Explicability. Transparency requires that the purpose, inputs, and operations of AI programs are knowable and understandable to its stakeholders. Transparency therefore impacts all elements relevant to an AI system: the data, the system and the processes by which it is designed and operated, as stakeholders must be able to understand the main concepts behind it (how, and for what purpose, these systems function and come to their decisions. Explicability means the transparency of Al processes and the capabilities, and it requires that the purpose of Al systems is openly communicated, and decisions – to the extent possible – explainable to those directly and indirectly affected.

Accountability by design, control and Oversight. Those who play an active role in the AI systems, e.g., in their development or operations, should take responsibility for the way that these systems function and for the resulting consequences and be accountable for the proper functioning of AI systems and for the respect of the above principles. To be held to account, developers or operators of AI systems



must be able to explain how and why a system exhibits characteristics or results in certain outcomes. Oversight entails that human actors can understand, supervise and control the design and operation of the AI system. Accountability depends on oversight: To be able to take responsibility and act upon it, developers and operators of AI systems must understand and control the functioning and outcomes of the system. Hence, to ensure accountability, developers must be able to explain how and why a system exhibits particular characteristics

6.2 Ethics Monitoring Mechanisms in SYNERGIES

In light of the discussion above, this section begins with analysing potential ethical considerations that pertain to the actual development of human-centric, secure and trustworthy data-driven technologies. Afterwards, it discusses the principles and rules of EU privacy and data protection laws which will be upheld by SYNERGIES. Finally, it elaborates on the technical and organisational mechanisms put forward under SYNERGIES allowing for Ethics Monitoring, therefore, providing in a timely manner for the identified ethics considerations and associated risks.

6.2.1 Ethical Considerations in SYNERGIES

The analysis on ethical considerations in SYNERGIES focusing on the deployment of two intertwined technologies, i.e., Big Data and AI. Because processing of data in mass by Machine Learning (ML) models to generate predictions and recommendations in energy domain is likely to have significant impacts over individuals' lives. Particularly, deploying AI systems without having effective data governance strategies in place is likely to cause potential disruptions in data processing activities which will eventually lead to a range of ethics risks. The most consequential forms in which these ethics risks manifest themselves are shown in the figure below:



Figure 5: Ethics Risks Related to AI-Driven Big Data Processing Activities

Denial of Individual Autonomy

SYNERGIES will collect a variety of data from individuals, i.e., prosumers, to run pilot activities. These range from contact details, information about homes and buildings, energy consumption, behavioural data, location data and personal opinions, for instance about comfort levels at home. During the data collection activities, individuals may feel that their instinct worth is compromised, and they become instrumentalized, objectified or dehumanized. Perhaps, use of a wide range of sensors and other IoT prevent individuals from participating in the entire data collection process: from identification of data needs; selecting appropriate collection tools; collection, analysis, and interpretation.



Furthermore, individuals control over the data might be very limited in AI-based systems following the collection. In particularly, the use of the ML solution that are built on non-transparent AI models may generate unexplainable results that are beyond the interpretive capabilities of human reasoning. In other words, the operator of the system may not be able to explain what data is being used, how it is being processed and why the system performed in the way it did in a specific context. When individuals are affected by the unfair decisions produced by these systems, these individuals become unable to hold directly accountable the parties responsible for the outcomes. In other words, prosumer affected by the AI system may be deprived of abilities to make basic decisions about fundamental personal issues (e.g. affecting directly private or professional life, health, well-being or individual rights), that are normally decided by humans by means of free personal choices; or about fundamental economic, social and political issues, that are normally decided by collective deliberations, or similarly significantly affects individuals. This prevents the affected individuals from exercising their right to recourse against such a decision and eventually restricts their autonomy.

Harms to Individual, Social and Environmental Well-being

Ineffective data governance models, flaws in general design of AI and improper deployment practices are likely to cause the AI systems to produce unreliable, unsafe, or poor-quality outcomes. These outcomes may unduly or unfairly reduce their psychological and emotional well-being. Al systems that can be deployed in the area of social and behavioural analytics or online communities and services may negatively impact the quality of social interaction, democratic processes, and social relations. The energy consumption of the system and the system itself and the supply chain to which it connects may also harm environmental well-being. In addition, it should be also noted that flawed AI systems eventually result in the loss of public trust toward the AI technologies due to the inefficiencies in terms of the allocation of limited public resources for the development of such flawed systems.

AI-Driven Bias and Discrimination

Bias and discrimination in the context of AI often result from the datasets used to train and facilitate algorithms. The datasets tend to reflect the existing structures, dynamics and disparities of the societies from which they were generated. Therefore, AI systems are prone to reproduce and amplify the patterns of marginalisation, inequality, and discrimination that are already exist in these societies. Unsupervised training of the AI systems with such data samples or the use of dataset that are insufficiently accurate and representative of the society from which they are drawing inferences inevitable create biased and discriminatory outcomes. In fact, the Council of Europe "Study on discrimination, artificial intelligence and algorithmic decision-making" offer the following taxonomy of AI-driven discrimination:¹²

Discrimination caused by target variable and class labels; In ML, the algorithm "learns" which attributes or activities can serve as potential proxies for certain qualities or outcomes of interest. Such an outcome of interest is called a target variable and class labels divide all possible values of the target variable into mutually exclusive categories.¹³ Importantly, the AI developers needs to translate a problem into formal computer coding, deciding on the target variable and the class labels is a subjective process. However, some target variables and class labels shaped by certain personal attributes such as wealth, gender or ethnicity may have a greater or lesser adverse impact on protected classes, such choice of class label would put people with a certain attribute at a disadvantage, even if they outperform others in other aspects. In other words, discrimination can creep into an AI system because of how an organisation defines the target variables and class labels.¹⁴

¹² Zuiderveen Borgesius, Frederick, Study on discrimination, artificial intelligence and algorithmic decision-making, Council of Europe, 2018 referring to Barocas, Solon and Selbst, Andrew D, Big Data's Disparate Impact, 2016, SSRN Electronic Journal ¹³ Ibid, 16.

¹⁴ Ibid, 17.



Discrimination caused by the biased training data; ML data analytics can also have discriminatory results if the model is developed from biased training data. If data is poorly labelled, inaccurate, incomplete or if it reflects human prejudices, then the ML model will reproduce those same biases.¹⁵

Discrimination based on feature selection; By selecting only certain features or attributes that an AI system uses for prediction; the organisation might introduce bias against certain groups.

Proxy discrimination; Some data that are included in the training set may correlate with protected characteristics and results in putting persons satisfying pre-defined rules or patterns of behaviour in a protected group at a particular disadvantage. Indirect discrimination does not focus on a particular individual but rather deals with rules or patterns of behaviour. It may be fair in form, but discriminatory in outcome. In machine learning contexts, indirect discrimination is considered the most relevant type of discrimination.¹⁶

Intentional discrimination; This is also called discrimination on purpose and it entails unfavourable or less favourable treatment on the ground of a certain characteristic such as race, sexual orientation, gender, religion or, sometimes, a combination of such characteristics. For example, a prejudiced designer could distort the training data or pick proxies for protected classes with the intent of generating discriminatory results.¹⁷

Invasion of Privacy

Deploying ML in big data analytics and processing of personal data may not always comply with lawfulness, data minimisation, purpose limitation, fairness and security principles under the GDPR. For example, Digital records of human behaviour may allow AI systems to infer not only individuals' preferences that is the original purpose conveyed to individuals concerned, but also their sexual orientation, age, gender, religious or political views. Furthermore, any unauthorised access to AI systems may allow malicious third parties to unauthorised access to personal data or to unlawfully process non-personal aggravated data in a way that reveals personal information that are not intended to disclose at the first place. Another threat to privacy is that the reliance on AI systems for the provision of public services may nudge individuals without their knowledge or consent toward certain behaviours that result in disclosure of more personal data.

6.2.2 Compliance with the EU Privacy and Data Protection Laws

When setting up a common energy data space such as SYNERGIES, privacy and data protection laws obviously need to receive special attention. With the big data and AI technologies, personal and nonpersonal data become increasingly intertwined so that SYNERGIES consortium understands that personal data would be processed at some point. Therefore, right from the beginning, SYNERGIES has been committed to high standards of information security, privacy and transparency and placed a high priority on protecting and managing personal data in accordance with ethical standards and data protection law, both at European and national level.

This section focuses on a certain data protection-related issues particularly relevant to common data spaces such as this of SYNERGIES. First, the definitions of certain key data protection terms and roles are briefly explained. Afterwards, the section continues discussing the data protection principles and the respective legal requirements. Finally, certain legal requirements under the E-Privacy Directive¹⁸ and the GDPR that are most relevant for SYNERGIES will be elaborated.

¹⁵ Ibid 17-18.

¹⁶ Ibid 21.

¹⁷ Ibid 22.

¹⁸ 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 (E-Privacy Directive)



Key Data Protection Terms

Personal Data is defined under the GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"¹⁹ Accordingly, in order to determine whether a natural person is identifiable, one should take into account all the means reasonably likely to be used, such as singling out, by any other person to identify the natural person directly or indirectly.

Special categories of personal data or sensitive personal data refers to certain types of personal data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural's sex life or sexual orientation"²⁰ The processing of such information is in principle prohibited, except in specific circumstances. For instance, if the processing is necessary for the purpose of medical diagnosis, or with specific safeguards in the field of employment law, or with explicit consent of the data subject, special categories of personal data can be processed.

Processing is another key term with a broad meaning. According to Art. 4 of GDPR, processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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".²¹ The important factor in the 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 personal data. 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 measures to ensure and demonstrate 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 in violation of the GDPR primarily falls on the data controllers.²²

Joint Controllership occurs in case where the determination of the purposes and means of a processing is made by two or more entities. 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.²³

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

¹⁹ Article 4(1) of the GDPR.

²⁰ Article 9(1) of the GDPR.

²¹ General Data Protection Regulation, Article 4(7).

²² General Data Protection Regulation, Article 82(2).

²³ Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, European Data Protection Board, 07 July 2021.



controller, and secondly, it processes personal data on behalf of the controller.²⁴ 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.²⁵ 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 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.²⁶

Due to this secondary role in data processing activities, processor's responsibility is rather limited than the data controller.²⁷ However, some of the more specific rules are addressed to both controllers and processors, such as the supervisory authorities' powers over data processors in Article 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 measures. In terms of liability toward individuals, processors shall be liable for the damage caused by processing only where it has failed to comply with obligations of the GDPR or where it has acted outside or contrary to lawful instructions of the controller.²⁸ 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 Article 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.

Pseudonymisation is a method for processing personal data and it "means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".²⁹ However, it should be noted that pseudonymised data still falls under the scope of the GDPR.

Anonymisation refers to processing of personal in such a manner that it does not relate to an identified or identifiable natural person (data subject) or that the data subject is not or no longer identifiable. Anonymised data does not fall under the scope of the GDPR because data which has been anonymised is no longer considered personal data.

Data Protection Principles in the GDPR

The GDPR is principle-based legal instrument and sets out seven (7) key principles which lie at the heart of the general data protection regime in the EU.

Lawfulness, fairness and transparency principle. This principle consists of three requirements. First, processing of personal data must be lawful. This means processing of personal data must rely on one

²⁴ General Data Protection Regulation, Article 4(8).

²⁵ General Data Protection Regulation, Article 28.

²⁶ Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, European Data Protection Board, 07 July 2021.

²⁷ General Data Protection Regulation, Article 24.

²⁸ Article 82(2) of the GDPR.

²⁹ Article 4(5) of the GDPR.



of the legal grounds stipulated under Article 6 of the GDPR and it should not do anything generally unlawful with the personal data. At least one of the following lawful bases for processing set out in Article 6 of the GDPR must apply whenever personal data is being processed:

(a) Consent: the individual has given clear consent for the processing of their personal data for a specific purpose.

(b) Contract: the processing is necessary for the performance of a contract between the data controller and the individual, or because it is necessary steps before entering into such a contract.

(c) Legal obligation: the processing is necessary for the data controller to comply with the law.

(d) Vital interests: the processing is necessary to protect the life of the individual concerned or someone else.

(e) Public task: the processing is necessary for the data controller to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for the legitimate interests of the data controller or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if the data controller is a public authority processing data to perform it's official tasks.).

Furthermore, lawfulness also means that the processing of personal data is not unlawful in the eyes of other regulations and legal obligations, whether criminal or civil. If processing involves committing a criminal offence, it will obviously be unlawful. However, processing may also be unlawful if it results in for example; a breach of a duty of confidence; organisation exceeding its legal powers or exercising those powers improperly; an infringement of copyright; a breach of an enforceable contractual agreement; or breach of sector-specific legislation or regulations.

The second requirement is that processing of personal data must always be fair. If any aspect of the processing is unfair, it will be in breach of this principle even if there is a lawful basis for the processing. In general, fairness means that personal data should be handled only in certain ways that individuals would reasonably expect and not use it in ways that have unjustified adverse effects on them. Assessing whether processing information is fair depends partly on how it is obtained. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair.

The last requirement of *transparency* is substantially linked to fairness. Transparent processing is about being clear, open and honest with those individuals whose personal data is processed, from the start about who the data controller is, and how and why the data controller uses their personal data. Transparency is always important, but especially in situations where individuals have a choice about whether they wish to enter into a relationship with the data controller. If individuals know at the outset what the data controller will use their information for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship. Under articles 13 and 14 of the GDPR, data controller is required to provide individuals with certain information about identity of the controller; contract details of data protection officer, the legal basis for the processing, the purpose of the processing, the recipients or categories of recipients of the personal data; the retention period of the personal data; existence of the data subject rights and information on how to exercise these rights; details of competent supervisory data protection authority and the existence of automated decision-making. Furthermore, this set of information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. In practice, privacy policies are used by controllers to fulfil the transparency requirements.³⁰

³⁰ Article 12 of the GDPR.



The purpose limitation principle requires that personal data must be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those initial purposes. In essence, if the purposes change over time or controller wants to use data for a new purpose which was not originally anticipated, personal data can be still processed only if: the new purpose is compatible with the original purpose; the individual whose personal data is subject to further processing provides specific consent for the new purpose; or there is a clear legal provision requiring or allowing the new processing in the public interest. The GDPR specifically says that the following purposes should be considered to be compatible purposes: archiving purposes in the public interest; scientific or historical research purposes; and statistical purposes.

The data minimisation principle requires personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Data controllers should identify the minimum amount of personal data they need to fulfil their purpose of processing and should hold only that much information. As a starting point, the use of personal data should be avoided by default; however, this is not always feasible for some operations. It is, therefore, crucial to design digital ecosystems as if these will at some point process personal data. A guiding principle when utilising personal data is to ensure that as much is used as necessary, but as little as possible to achieve the desired outcome.

The accuracy principle requires personal data to be accurate and where necessary, kept up to date and data controller take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In practice, this principle requires data controllers to take reasonable steps to ensure the accuracy of any personal data and that the source and status of personal data is clear. In that regard, the data controller should carefully consider any challenges to the accuracy of information and consider whether it is necessary to periodically update the personal data that have already been stored. Furthermore, in relation to this principle, article 16 of the GDPR provides for the right to rectification which gives individuals the right to have inaccurate personal data corrected by the data controller.

The storage limitation principle simply requires data controllers to keep the personal data no longer than what is necessary for achieving the purposes for which the personal data is processed. It is vital that the controller knows exactly what personal data it processes and why. The purpose of the processing shall be the main criterion to decide in how long personal data shall be stored. Measures and safeguards that implement the principle of storage limitation shall complement the rights and freedoms of the data subjects, specifically, the right to erasure and the right to object. Key design and default storage limitation elements may include, for example, deletion and anonymization of personal data following the completion of the processing or implementing deletion procedure and binding storage criteria which determine what data and length of storage is necessary for the purpose and when the data will be deleted automatically.³¹

The integrity and confidentiality principle includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The principle manifests itself as legal requirement for the security of personal data under Article 32 of the GDPR. It requires appropriate measures designed to prevent and manage data breach incidents; to guarantee the proper execution of data processing tasks, and compliance with the other principles; and to facilitate the effective exercise of individuals' rights. The GDPR puts responsibility on the controllers to continually assess whether it is using the appropriate means of processing at all times and to assess whether the chosen measures actually counter the existing vulnerabilities. Furthermore, controllers should conduct regular reviews of the information security measures that surround and protect personal data, and the procedure for handling data breaches. Key integrity and confidentiality elements may include pseudonymisation of personal data,

³¹ European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, 20 October 2020.

establishing security incident response management procedures, disaster recovery and business continuity plans, keep back-ups and logs to the extent necessary for information security and carrying out risk analysis.

The accountability principle requires the data controller to be responsible for and be able to demonstrate compliance with all of the abovementioned principles. In doing so, the controller may demonstrate the effects of the measures taken to protect the data subjects' rights, and why the measures are considered to be appropriate and effective. For example, demonstrating why a measure is appropriate to ensure the principle of storage limitation in an effective manner. To be able to process personal data responsibly, the controller should have both the knowledge of and the ability to implement data protection. This entails a number of legal requirements including but limited to designating data protection officer,³² conducting prior data protection impact assessment,³³ keeping records of processing activities,³⁴ executing a written data processing agreement with data processor³⁵ and notifying competent data protection authorities of a personal data breach^{36.}

Key Requirements under the GDPR and the E-Privacy Directive

Having a valid legal basis for the processing of personal data. Data controller should not commence processing of personal data before identifying a valid legal basis. If no lawful basis applies to the processing, it will be deemed unlawful and in breach of the GDPR. Considering the purpose and the context of processing activities in the SYNERGIES project, three potential legal bases can be relied on. The first option can be the legitimate interests pursued by the SYNERGIES consortium according to Article 6(1)(f) of the GDPR. Because in order to create a reference common European data space, the processing of data related to energy consumption of households or electricity generation by the prosumers is inevitable and prosumers and the society in general would benefit greatly from this processing. However, the partners acting as data controller should still carry out a weighted balancing of interest, giving particular attention to the power imbalance, specifically children under the age of 18 and other vulnerable groups impacted by the project. Therefore, the partners will implement measures and safeguards to mitigate the negative impact on the individuals. Secondly, the contractual relation with individuals for the provision of data-driven, AI-powered energy services on the SYNERGIES platform could be accepted as a legal basis for personal data. However, the partners will only rely on this ground if the processing is absolutely necessary or the only way for the partners to perform their obligations under the service contract or to take relevant pre-contractual steps such as signing in the platform.³⁷

In fact, consent may also serve as a legal basis for collecting data from prosumers participating the energy data space. Consent for the processing of personal data should meet the criteria stipulated under Article 7 of the GDPR, namely that it has been provided unambiguously, it was informed, free and not conditional on the provision of services. Furthermore, individuals can withdraw their consent at any time and once withdrawn, the data controller should immediately delete the data and terminate data processing activities. Therefore, the consent is generally considered as the last option for long-term processing activities. Moreover, it should be noted that the processing of personal data in connection with the provision of publicly available electronic communications services³⁸, including

³⁵ Article 28 of the GDPR

³² Article 37 of the GDPR

³³ Article 35 of the GDPR

³⁴ Article 30 of the GDPR.

³⁶ Article 33 of the GDPR

³⁷ European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 16 October 2019.

³⁸ For example, the internet or mobile phone networks can be considered as publicly available electronic communication services in accordance with the EDPD's Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR.



placing and retrieving information like IP addresses through the cookie or similar device or processing of IoT communication content data and possibly metadata trigger the material scope of e-Privacy Directive. In other words, accessing and processing of personal data which have been stored in the prosumers' smart devices for example metadata related to energy consumption stored in smart meters, location data stored in the vehicle require prior consent of the prosumers concerned according to Articles 5(3) and 9 of ePrivacy Directive.³⁹ Reading the ePrivacy Directive and the GDPR together, it can be concluded that data controller to obtain prior consent of individuals in order to access the personal data stored in personal smart devices.⁴⁰

Data Protection Impact Assessment. 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".⁴¹ This means that data controller is only required to carry out a DPIA if the 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", in its Guidelines on Data Protection Impact Assessment, the European Data Protection Board (EDPB) provides data controllers with a list of nine (9) criteria together with some examples.⁴² 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 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 require the data controller to conduct a DPIA. It should be further noted that even if the envisaged processing operations is not likely to result in a high risk, DPIA could be useful for the project partners for identifying the risks arising from their data processing activities. In that regard, it is thus suggested, in particular for the demo site leading partners, to carry out a risk assessment with respect to their processing activities. This will allow the 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 in a timely manner.

Furthermore, individuals whose personal data is processed should be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR and the data controller should provide a set of information, i.e. privacy notice, as explained above with respect to the transparency principle. The individuals should be informed at the time their personal data is collected from them.⁴³ If their personal data obtained from other sources, they receive privacy notice within a reasonable period of obtaining the data and no later than one month.⁴⁴Finally, identification of the roles of data controller and processor in the project consortium is also crucial for the project's compliance with the GDPR. In case it is determined that some partners will act as data processor on behalf of other partners acting as data controller, data processing agreement between these partners, i.e. data controller and processor, should be executed in accordance with Article 28 of the GDPR. Such agreement is also recommended in case where two or more partners acting as joint controllers.

⁴³ Article 13 of the GDPR.<u>https://intellectual-property-helpdesk.ec.europa.eu/horizon-ip-scan_en</u>

³⁹ ePrivacy Directive, Articles 5 and 9.

⁴⁰ 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.

⁴¹ 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.

⁴² European Data Protection Board, 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.

⁴⁴ Article 14 of the GDPR.



6.2.3 Organisational Mechanisms

The SYNERGIES Ethics Monitoring includes several organisational mechanisms to mitigate the ethics risks identified above.

Establishing Citizen-Oriented and Democratic Data Governance

SYNERGIES aims at building a sense of empowerment among prosumers, whose voices and opinions are valued and taken into account in the planning, execution, and validation of the project. The partners commit to ensuring that participants are informed, understand, and agree on the purpose of data processing. The project will offer the participants relevant information to make their participation genuine and communicate clearly using language everyone can understand.

Furthermore, SYNERGIES aims to equalize power relations and receive the opinions of all groups in order to shape co-creation work from different perspectives. It is important to avoid looking at participants as only research/data subjects and presenting the consortium partners as the experts on the subject as it may generate an unwanted imbalance in power relations. Therefore, SYNERGIES will take into account everybody's thoughts as valuable assets and allow participants to provide feedback on how project outcomes influenced them. It will offer participants the opportunity and the means to exercise active governance over their data: e.g., decide which data to grant and under which condition, discuss the fate of the data when the project is finalised, etc

Embracing Ethics by Design Approach

SYNERGIES put forward the "Ethics by Design" approach as defined under the EU Commission's Guidance on Ethics by Design and Ethics of Use Approaches for Artificial Intelligence. This design approach for AI systems enables the technical project partners to incorporate ethical values, principles and requirements into the design and the development processes of AI-driven services. The goal of this approach is to address the ethical issues as early as possible and follow up them closely during the entire development and deployment processes of the systems. According to the European Commission's guidelines, Ethics by Design approach consists of five layers as illustrated in the figure below;





Figure 6: The 5-layer Model of Ethics by Design⁴⁵

This five-layer model is the first step that helps the developer to map and plot own development methods based on identified ethics values and requirements. Afterwards, a generic model containing six phases will be followed by the developers and data scientists to properly embed Ethics by Design in the development processes. These six phases refer to the specific points in the AI development methodology in which the ethical requirements need to be instantiated as tasks, goals, constraints, and measures to prevent ethical risks arising in the first place. Although the six phases of the generic model under the Ethics by Design approach are illustrated in a list format below, the European Commission explicitly states that it is not a sequential process, and the developers and data scientists are advised to tailor these phases into the similar steps in their chosen development methodology.

⁴⁵ The content of the figure is largely based on the information provided under the EU Commission's Guidance on Ethics by Design and Ethics of Use Approaches for Artificial Intelligence of 25 November 2021 and under the Deliverable Report of Ethics by Design and Ethics of Use in AI and Robotics published by the EU-funded SIENNA project.





Figure 7: The European Commission's Generic Model for AI Development⁴⁶

It should be noted that each of these steps includes different tasks which must be undertaken by the developers and data scientists in order to ensure ethics compliance of their AI systems.⁴⁷

Conducting Ethics Self-Assessment

Acknowledging both the benefits and the risks associated to the use of AI in big data, SYNERGIES assigns ethics assessment and monitoring with a key role throughout the project. The objective is to prevent the AI systems deployed within the project from unintentionally or intentionally creating any ethics risk by way of, for instance, creating social disadvantages to people either by the AI-based system, or by the way it will be deployed.

In this respect and building on the European Commission's Guidelines on Ethics by Design and Ethics of Use Approaches for Artificial Intelligence, SYNERGIES provides for a methodology on ethics selfassessment focusing on the following areas: 1) AI Human Agency and Oversight, 2) Technical Robustness and Safety, 3) Privacy and Data Governance, 4) Transparency, 5) Diversity, Nondiscrimination and Fairness, 6) Societal and Environmental well-being and 7) Accountability. Moreover, it will require the SYNERGIES consortium to assess periodically AI-based technologies at different stages of the AI lifecycle, particularly, on the identification and discussion of ethical issues and tensions through the elaboration of socio-technical scenarios and to address these issues accordingly. To this end, SYNERGIES will produce necessary tools for such self-assessment such as ethics assessment guidelines that can enable the partners and participants to carry out ex-post conformity assessments at regular intervals, throughout the AI lifecycle in order to protect citizens and environment from potential harms, while reducing the costs incurred for the partners. Within the scopes of the tasks T2.4 "Architecture Design and Technical Specifications" and T2.3 "Analysis of Regulatory and Socio-economic Barriers", the consortium will develop ethics self-assessment procedures including covering data protection, ethics and human rights impact assessments. These templates will provide clear definitions of some important terms such as AI, provider of AI systems, user of AI systems, data controller, data processor and end user and identify important ethical requirements. The assessment will further facilitate the development of trustworthy AI systems within

⁴⁶ The six phases of the generic model shown in the Figure-2 is based on the illustration provided under the EU Commission's Guidance on Ethics by Design and Ethics of Use Approaches for Artificial Intelligence of 25 November 2021

⁴⁷ Further detailed discussion and explanation of each specific tasks under the six phases of the generic model can be found in the EU Commission's Guidance on Ethics by Design and Ethics of Use Approaches for Artificial Intelligence of 25 November 2021 as well as in the Deliverable report of Ethics by Design and Ethics of Use in AI and Robotics published by the EU-funded SIENNA project in 2020.

the scopes of the tasks T2.4 "Architecture Design and Technical Specifications" and T2.3 "Analysis of Regulatory and Socio-economic Barriers" devoted to the ethical assessment of the sociotechnical solution.

In particular, the assessment will pose generic questions to identify the objective, the proportionality of the technique chosen, the stakeholders, their roles and respective responsibilities on a case-by-case basis. Specific questions will be then raised per use cases. For instance, in relation to the privacy and data governance, particular attention will be given to assessment of compliance with the GDPR, especially, in relation to the origin of the data, on the actual possibility of reusing it for training purposes or on the measures taken to limit the risks of misuse. Moreover, in line with the prior data protection impact assessment requirements under Article 35 of GDPR, the assessment will further focus on the design and choice of algorithm, tools and development infrastructure (supervised, unsupervised, continuous or federated learning, learning by reinforcement, etc.). The questions raised in the template for the ethics self-assessment will be in the spirit of upcoming EU legislative initiatives, i.e., AI Act, while considering guidelines by Data Protection Authorities such as those recently published by Commission Nationale de l'Informatique et des Libertés's "Self-assessment Guide for AI systems, AI: ensuring GDPR compliance".

Afterwards, in order to properly address the identified risks, SYNERGIES will modify or reconfigure the elements of the AI design and to implement the measures and procedures in the development process in accordance with the Ethics by Design approach.

6.2.4 Technical Mechanisms

Certain technical developments within SYNERGIES aim to, among other, support the effectiveness of the organizational mechanisms discussed, therefore, contributing to the mitigation of the abovementioned ethical considerations. First, the SYNERGIES Living Lab which will be set up within Tasks T6.1 will be used to communicate the purpose and procedure of the project to the prosumers in a concise, transparent, intelligible and easily accessible way. It will be emphasized that it is the prosumers' choice about whether to get involved in the SYNERGIES project. All prosumers will be informed, through the SYNERGIES Living Lab, of their right to privacy and the extent to which participation in this project may impact on their lives and the mechanisms the consortium have put in place to protect privacy through processes of data privacy preservation, security and modality of storage. Furthermore, interviews and group discussions will be organized under the SYNERGIES Living Lab to capture the views and feedbacks from the prosumers.

Secondly, the SYNERGIES Data Security and Sovereignty Block will enable prosumers to remain in control of their data by defining with whom these can be shared, for example, via access control policies, the privacy methods applied over them and the modality to store them in their private/edge infrastructures, thus safeguarding security of collected personal data from potential abuse, theft, or loss. Basically, this block supports the privacy by design approach in the development of the SYNERGIES reference common energy data space.

Thirdly, the SYNEGIES Trusted Data Sharing Block and blockchain-based smart contracts will provide the means to prosumers to enter into data sharing agreements that will allow them to continuously track the life cycle of their data. Smart contract further enables the prosumer to monitor if their data are used in a non-legitimate manner which could automatically terminate the contract and access of external stakeholders to the data assets of prosumers. Prosumers will be able to exercise their data subject rights set out between Articles 12 - 22 of the GDPR to the extent possible and they can withdraw from the project at any time and that they have the right to stop providing access to their personal data.

7 SYNERGIES Approach to IPR Management

Intellectual property (IP) is the collective name of exclusive rights that protect intellectual creations of humans usually for a certain period. Generally, IP rights (IPRs) are divided into two main areas: industrial property which includes patents, trademarks, industrial designs and models and designations of origin, and copyrights and rights related to copyright, which includes artistic and literary property and any other legally protectable information, including computer program, database.⁴⁸ However, in addition to these two categories, there are sui generis right given to persons over a database that is not deemed as an intellectual creation under copyright law but still protects against the re-using of data in that databases and also trade secrets which allows businesses and individuals to keep business information, whether or not defined as part of IPR, confidential indefinitely.⁴⁹ It should be noted that to entitle for some of these IRPs, such as trademark, patent, design rights, the right holder must register or deposit whereas other IPRs such as copyright, database rights are gained automatically. Bear in mind that, regardless of whether registration is required, when it comes to claiming IPRs, it is always best to have a written record that identify the owner of the IPR of a product or service concerned.

In today's economy, digital products and data-driven processes increasingly rely on intangibles protected by IPRs and other related rights notably copyright, sui generis right, patent, trade secrets and therefore, strong IP management has become a must-have part of any successful business initiative. In that regard, SYNERGIES aims to increase the consortium partners' awareness of relevant IPRs and to implement a solid IP management mechanism as one of the critical foundation of SYNERGIES Energy Data Space which will enable successful exploitation and market deployment of the wide range of SYNERGIES outcomes. Therefore, the SYNERGIES consortium places great emphasis in managing innovation and IPR in the framework of the project, with a view to effectively paving the way for the smooth exploitation and sustainability of its results following its completion.

As described under the SYNERGIES Grant Agreement⁵⁰ (GA), the present deliverable provides the SYNERGIES consortium with tailored guidelines on IPRs management in SYNERGIES. The guideline will embrace the need to protect project's assets to handle and provides insights into the IP landscape in SYNERGIES to enable the consortium to manage efficiently all the outcomes that will stem during the project's life span with a view to ensure the commercial rollout of the exploitable results along with their proper dissemination. In that regard, this chapter begins with the description of the state of play of the IPR Management in SYNERGIES where the legal framework for possible IPRs in SYNERGIES is explained. Afterwards, the chapter carries out an analysis of the key elements in SYNERGIES IPR Management and provide guidance on how to protect IPRs in SYNERGIES. Lastly, this chapter concludes by defining a methodology for IPR management in SYNERGIES that will be followed by the consortium partners throughout the life cycle of the project.

7.1 State of Play in SYNERGIES IPR Management

IPR Management in SYNERGIES is currently governed by the provisions of the GA and the SYNERGIES Consortium Agreement⁵¹ (CA) concerning ownership and access rights over the assets envisaged to be

⁴⁸ European Parliament, Intellectual, Fact Sheet on Industrial And Commercial Property, 2022 available at <u>https://www.europarl.europa.eu/factsheets/en/sheet/36/intellectual-industrial-and-commercial-property#:~:text=Intellectual%20property%20includes%20all%20exclusive,includes%20artistic%20and%20literary%20prop</u>

<u>erty</u>.

⁴⁹ European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Making the most of the EU's innovative potential, COM(2020) 760 final, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760#footnoteref2 ⁵⁰ SYNERGIES, Grant Agreement No 101069839, 31 March 2022.

⁵¹ SYNERGIES, Consortium Agreement, 9 March 2022.

used or generated within the SYNERGIES project as well as by the EU laws on IPR protection that are relevant to these assets.

7.1.1 Internal Documents Regulating the IPRs in SYNERGIES

Under the GA and the CA, the SYNERGIES partners agreed on the binding rules regulating the ownership and the IPRs for three (3) categories of assets, i.e., background, results and software. Particularly, the rules on "access rights" referring to rights to use these assets by the partners constitute a fundamental part of the current SYNERGIES IPR management. However, due to the confidentiality of the content of these agreements, this section confines its content to a high-level overview based on corresponding provisions of publicly available the EU Annotated Model Grant Agreement designed for EU Funding Programmes (hereinafter referred as 'Model GA')⁵² and the DESCA Model Consortium Agreement⁵³ (hereinafter referred as 'Model CA') since these model agreements are the basis of the SYNERGIES GA and CA respectively.

Background

Background as defined in Article 16 of the Model GA mean any data, know-how or information whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights held by the respective partner before it acceded to the GA and needed to implement the action or exploit the results.⁵⁴ In line with this provision, under Attachment 1 of the CA, the partners have identified and agreed on the Background for SYNERGIES and have also, where relevant, informed each other of the legal restrictions and limits to which access rights to Background are subject.⁵⁵ The details of the conditions and restrictions with respect to the partners' IPRs on Background can be found in Attachment 1 of the CA.

Results

As defined in Article 16.2 of the Model GA, Results means any tangible or intangible effect of the project, such as data, know-how or information, whatever its form or nature, whether it can be protected or not, as well as any rights attached to it, including intellectual property rights. Pursuant to Annex 5 of the Model GA and Section 8 of the Model CA, Results are generally owned by the partner that generates them. However, the model CA also allows joint ownership of a Result if i) two or more partners have jointly generated it and ii) it is not possible to a) establish the respective contribution of each partner, or b) separate them for the purpose of applying for, obtaining or maintaining their protection.⁵⁶ To comply with the respective obligations arising from the GA, the joint ownership. It is important to note that in line with the principle *'as open as possible, as closed as necessary'*, the model CA allows each of the joint owners to use their jointly owned Results for non-commercial research and teaching activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s). It further allows the joint owners individually exploit Results based on fair and reasonable compensation.⁵⁷

Software

Specific rules on access rights to software is stipulated in Article 9 of the Model CA. In line with the model CA, the SYNERGIES partners have agreed on the rules under the SYNERGIES CA that regulate the access rights to software including both software brought by a partner as background and those will be developed within the project. Furthermore, the SYNERGIES CA includes further detailed

⁵⁵ DESCA for Horizon Europe model CA version 1.0, July 2022.

⁵²European Commission, EU Grants AGA – Annotated Model Grant Agreement, 20 November 2021.

⁵³ DESCA for Horizon Europe model CA version 1.0, July 2022. Available at <u>https://www.desca-agreement.eu/desca-model-consortium-agreement/</u>

⁵⁴ European Commission, EU Grants AGA – Annotated Model Grant Agreement, 20 November 2021

⁵⁶ Ibid, Section 8.

⁵⁷ Ibid.

provisions concerning the conditions for granting access rights of the project partners to source code, object code and API that is either developed by the project or brought by the other partners.

7.1.2 Relevant European IP Laws

IP management plays an essential part in the entire lifecycle of research and innovation projects funded by the European Commission's Horizon Programme and the EU Regulation No 2021/695 establishing Horizon Europe – the Framework Programme for Research and Innovation⁵⁸ encourages the partners to make use of the relevant existing Union's instruments in both protecting and enforcing their IPRs. In fact, Article 39 of the Regulation requires the EU funded projects to disseminate results and to grant open access to the research outputs in compliance with the applicable EU laws on IP. Therefore, it is important to identify IPRs which could be of direct relevance to SYNERGIES outcomes, i.e., datasets and software and the applicable EU laws.

Data

As the title speaks for itself, data is a backbone of SYNERGIES Energy Data Space, and it will be shared and processed by the project in order to offer envisaged AI-supported services. Due to the project's dependencies on data, the IPRs over data have significant impact on the project activities.

In general, raw research data is usually not protected by IP rights as such data is not considered as an intellectual creation of human mind. Under certain conditions, it could be considered as trade secrecy. However, under special circumstances, data in a certain form may display a certain level of originality and intellectual creativity, and therefore become subject to the protection under the copyright law in the EU. In that regard, data structured in an original way, e.g., database, is likely be protected as an original intellectual creation through copyright which guarantees the creator exclusive rights to reproduce, adapt, distribute the database or any variation of it under the EU Database Directive.⁵⁹ However, it should be noted that with copyright, the protected work is not the content but the structure of database. Therefore, raw research data can be protected as long as it forms a database in the legal sense. Furthermore, as a rule, only the natural person or group of natural persons who created the database can be the copyright holder. However, where the legislation of the Member States permits, the legal person can also be designated as the right holder by that legislation.⁶⁰

If the structure of database is not an original creation which means that it does not carry the creativity or originality of its maker, it cannot be protected under copyrights. However, Article 7 of the Database Directive still provide for certain level of procreation for such under sui generis right. Sui generis right is often used to protect big data that does not have the level of originality required for copyright protection. Sui generis right is different to copyright, but it provides for limited protection for database compared to copyright. To benefit from sui generis protection, it must be proved that the creator of the database has made a substantial investment (financial, material and/or human) in either, obtaining, the verification or the presentation of the database content. The right holder can prevent the extraction and/or reuse of the whole or a substantial part of the database's content.⁶¹ When the databased is created and it meets the investment requirements for the sui generis rights, the protection is granted for 15 years, starting either from the creation date or from when the database

⁵⁸ Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013, OJ L 170/1.

⁵⁹ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 077/20 amended by Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130/70 (Database Directive).

⁶⁰ Database Directive, Article 4.

⁶¹ Database Directive, Article 7.



was first made publicly available.⁶² In case of a protected database, third parties must request permission from the creator before: retrieving or copying or downloading substantial parts of the database; repeatedly and systematically retrieving non-substantial parts of the database; or reusing or publishing substantial parts of the database. On the other hand, according to Article 8(1) of the Directive, permission is not required for extracting and/or re-utilizing insubstantial parts of the contents of a publicly available protected database, provided that such use does not unreasonable prejudice the legitimate interest of the creator. Furthermore, use of a substantial part of a publicly available protected database for teaching or scientific research purposes are allowed as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved.⁶³

Last but not least, the European Commission's proposal for the Data Act⁶⁴ will also have impact on sui generis protection of databases. According to Article 34 of the proposal, the sui generis right under the Database Directive does not apply to databases containing data generated or obtained by the use of internet of things (IoT) or related services. The proposal aims to ensure that the sui generis right will not interfere with rights for businesses and consumers generating data through their uses of IoTs to access and use such data and to share it. Undoubtedly, this restriction to the scope of sui generis rights will facilitate data sharing and have a positive impact on the uniform application of rules in the internal market and for the data economy.

Software

Stand-alone software can be protected under the Computer Programs Directive⁶⁵. According to Article 1 of the Directive, software, AI models or code of a computer programme in any form including the preparatory design material, machine code, source code and object code are protected as literary works by copyright across the EU if it is deemed original in the sense that it is the author's own intellectual creation.⁶⁶ However, ideas and principles which underlie a computer program or any elements of it such as functionality of a program or data format are not under the scope of this protection.⁶⁷ Like in copyrights over the database, the right holder can be the natural person or group of natural persons who has created the program or, where the legislation of the Member States permits, the legal person designated as the right-holder by that legislation. If several persons participate in creating a program, the exclusive rights are held jointly by these persons. The holder of the rights to a computer program may do, or may authorise others to do, the permanent or temporary reproduction of the program, or a part thereof; the translation, adaptation, arrangement and any other alteration of the program; and the distribution of the programme.⁶⁸ According to Article 6 of the directive, prior authorisation from the rights-holder is not required where reproduction of the code and translation of its form are essential to obtain information necessary to achieve the interoperability of a new computer program with other programs. However, this action will be subject to the following conditions; i) those acts are performed by the licensee or another person having a right to use a copy of a program; ii) the information on interoperability has not previously been readily available; and iii) those acts are confined to the parts of the original program which are necessary in order to achieve interoperability.

⁶² Database Directive, Article 10.

⁶³ Database Directive, Article 9.

⁶⁴ 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, available at https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

⁶⁵ Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111/16. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0024.

⁶⁶ For the broad interpretation of "computer program" by the Court of Justice of the European Union, please see the case SAS Institute C-406/10.

⁶⁷ Computer Programs Directive, Article 1.

⁶⁸ Computer Programs Directive, Article 4.


In addition, any products using computer software or software-related inventions can be protected by patent. A patent is an exclusive right granted for an invention, which is a product or a process that provides a new way of doing something or offers a new technical solution to a problem. Therefore, software as such is excluded from patent protection. However, if software presents as a method or a system of methods or as a technical means implementing a method which provides a solution to a technical problem in a certain technical domain, such software can be subject to patent protection. Image processing, data compression, noise suppression, encoding software or the control software of industrial process or energy grid may be examples of potentially patentable software.⁶⁹

7.1.3 Key Concepts in SYNERGIES IPR Management

As a first step towards proper IPR management, the project partners need to be aware of the subjects of the potential IPRs in SYNERGIES, the stakeholders and the legal arrangement with respect to use of the identified IPRs. Therefore, this section concludes with identifying and analysing potential IP terminologies within SYNERGIES as to provide the partners with necessary awareness.

SYNERGIES introduces a reference energy data space implementation which will facilitate the integration of the energy data value chain and the creation of an inclusive ecosystem of stakeholders around energy data and intelligence. The stakeholders of SYNERGIES Energy Data Space are data asset owners or providers who expose their data either at batch level or as real-time / streams via appropriately defined APIs, end-points and connectors and data asset consumers who expresses their data needs, discovering the requested data (intelligence) assets, negotiating on the terms for their acquisition (in a bilateral manner with data asset providers, or multi-lateral in the case of derivative data sharing) and establishing fair and objective data asset sharing agreements, safeguarded by secure and transparent data contracts, stored, monitored, managed and settled in a blockchain infrastructure or providers data asset. On top of this dynamic energy data space, SYNERGIES will develop and offer novel AI analytics applications to analyse and extract data-driven intelligence and valuable knowledge generated by data produced across the different edges of the energy system within the same energy data space and to offer the fundamental intelligence to be further elaborated in the optimization functions of the energy services and applications. Finally, SYNERGIES implements digital twins to effectively address and optimize business operations of certain stakeholders across different levels of the energy system. However, it is noted that the digital twins will be built on the existing tools as Background offered by the technical partners involved through granting a free, non-transferrable license. In this dynamic and complex data ecosystem, it becomes evident that following technologies, concepts and stakeholders will play key roles in SYNERGIES IPR Management.

SYNERGIES Network of Sectorial Data Models. The SYNERGIES Energy Data Space contains three (3) connected sectorial data models, i.e., energy, buildings and mobility data models, which will be built on most prominent open standards, semantic models and ontologies in SYNERGIES. These data models to the extent that they are function as data management system, could be considered as technical systems implemented on computers to perform the technical tasks of storing and retrieving data using various data structures for efficient management of data in SYNERGIES Energy Data Space. A method performed in a database management system is thus a method which uses technical means and is therefore not excluded from patentability.⁷⁰

Data Assets. If these data assets function as database that contain structured raw energy, building and mobility data and shared with the SYNERGIES Energy Data Space, they could be subject to sui generis rights or copyrights as explained in the previous section.

SYNERGIES Energy Data Space. To a certain extent, the SYNERGIES Energy Data Space is likely to act as a novel data management system and method for energy data providing a solution to a technical

⁶⁹ Pasa, Barbara, Copyright and Data Protection, In book: Privacy and Data Protection in Software Services (pp.111-123), January 2022.

⁷⁰ European Patent Office, Guidelines for Examination, Part G Patentability, March 2022.

problem in energy domain, i.e. interoperability and meaningful data governance and thus could be considered under patent law.

Al Analytics application. These may qualify as computer programs under the Computer Programs Directive and as stand-alone application might benefit from copyright protection. However, together with SYNERGIES Energy Data Space framework, they could constitute a patentable product.

Data Asset Owners. Depending on the content of data assets whether it is a database or not, data assets owners might qualify as the right holders of sui generis or copyrights. However, if data assets refer to raw data to be collected from prosumers participated to SYNERGIES, then these prosumers may not be considered as IPR holders.

Data Asset Providers. According to the SYNERGIES project DoA, data assets providers will be businesses that collect data from data assets owners and then structure or curate these data in a certain way that is compatible to the SYNERGIES Energy Data Space.

Data Asset Consumers. According to the SYNERGIES project DoA, the role of data asset consumers has two facets. On the one side, these are business that need to have access to fine-grained, high quality, interoperable data or datasets in order to utilise their data-driven operations and to deliver intelligence and innovative energy services across the SYNERGIES value chain. From this perspective, data asset consumers will act as licensor which is legally entitled to access datasets provided by data asset providers. On the other side, the outcome generated through the provision of their intelligence and innovative service could also be subject to IPRs and thus, they could become the right holders of potential IPRs on their services.

Smart Contracts. These are simply computer programs that run on decentralised ledger technologies that are intended to automatically execute, control or document mutual exchange of the data assets and corresponding remuneration at specific granularity levels and time frames according to the terms of a legally binding contract or an agreement executed by the data assets providers and data assets.

These code-based smart contracts can facilitate the enforcement of a legally binding contracts, i.e., data sharing contracts, that have been executed by the stakeholders. Smart contracts themselves, though, cannot provide the legal basis allowing for the exchange of IP protected data assets .

7.2 SYNERGIES IPR Methodology

The SYNERGIES IPR Methodology starts with drawing a concrete IP mapping and planning of the IP assets including those expected to be developed within the project. These assets will be identified, listed, named and analysed, in a systematic way, to have a sort of project IP portfolio. For this purpose, the SYNERGIES consortium may need to create a separate IPR folder in the project repository. This folder will eventually represent the living IPR database during the project's implementation and it facilitates the identification and licensing project intangibles and documentation of their ownership, being also functional to help the partners to recognize their IP assets and ascertain the existence of third parties' rights.

Moreover, with respect to the project result, key elements such as which partner(s) are directly contributing to its development, which background is needed and used to develop the result, rights to use such result and license scheme will be identified throughout the project life cycles. The strong and continuous collaboration and communication between partners are crucial for IPR management. Therefore, during the project meetings that will be held at regular intervals, the partners are expected to inform the coordinator and others of any new results and envisaged allocation of IPRs generated over such results in the context of the WP6 activities. This will open the way for a further identification of those exploitable results and will allow the SYNERGIES partners to have the most complete information to decide about their sustainability once the project is finished. The strong and continuous collaboration between partners are crucial for IPR management.



To ensure the efficient management of IPRs, it is advisable to adopt a timely process able to discuss and agree on their handling and protection following the identification. Because protecting IP has several benefits. First, it protects an invention, such as a result. Directly the owner becomes the only person with the right to use or reproduce it. Others cannot copy or reproduce what this invention is ensuring without the owner's permission. Secondly, in some cases, such as for copyright and sui generis right, protecting IP is automatic and doesn't require any formalities. In this way, the partners can immediately start exercising their IPRs over the data and data-driven services and they can guarantee the quality of the data and the related service. This can be an advantage for businesses because users may prefer to receive services or products that have already passed more restrictive checks. Moreover, not only through direct use of IP, but also indirectly through licensing contracts can produce more benefit to the partner and the EU in general. This occurs when the owner grants a licence to another company to use the IP protected subject matter for a certain period.

Since the partners mutually agree on co-ownership based on the actual partner contribution in the design and development of the result, appropriate IPR protection measures will be also selected by the joint owners partners. In that regard, the partners are invited to mobilize services provided by the European Commission IP Helpdesk⁷¹ and more specifically the Horizon IP Scan⁷² service to facilitate the development of a joint IP management strategy and prevent potential IP conflicts and boost plan for the exploitation.

In light of above, this section below continues to explain envisaged measures for IPR protection in SYNERGIES and then elaborates on legal ground for data sharing in the SYNERGIES framework, i.e. data sharing contract.

7.2.1 IPR Protection in SYNERGIES

EU Directives on database and computer programs and the respective national implementations of the directives provide for significant legal protection for IPRs in SYNERGIES in the EU. By building upon these laws, the relevant sections of the GA and the CA grants further rights of ownership and rights to use IPRs. However, SYNERGIES still need to use a large amount of raw data and databases that may not fall into scope of copyright protection, because they might be deemed as creative or original like an author's work. In principle, therefore, the exchange of such raw data cannot be protected by the usual IPR protection mechanisms. In addition, sui generis protection for databases that do not meet the conditions for copyright protection is subject to a vague condition of having spent "a substantial" investment in creation of such databases. The vague terminology makes it difficult for the creators to exercise their rights over databases. Furthermore, sui generis protection for a database only prevents a third party from using a "substantial" part of the contents and again determination of "substantial part" is often very blur for the stakeholders. Given that the weaker protection for data compared to other IPRs, the following options will be implemented to support the IPR protection in a common data space and digital platform like the SYNERGIES framework:

- Protection through (user) contracts for the use of data-driven AI-powered energy services on • the online platform
- Protection through smart contract-based exchange mechanism of data •
- Protection through technical security systems for transmission, storage and access •
- Protection through monitoring of data quality and transmissions, corresponding alarm mechanisms and certification for trusted data sources
- Protection through encryption of data

¹¹ Available at https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk_en.

⁷² Available at <u>https://intellectual-property-helpdesk.ec.europa.eu/horizon-ip-scan_en</u>



No	Measures	Description
1.	Terms and Conditions	Protecting IPR over data and database by entering user contracts with the users of the SYNERGIES platform. IPR issues are integrated into these at the contractual level and sanctioned by, for example, contractual penalty in the event of abuse.
2.	Contract-based exchange mechanisms to data	Linking access to data sets by means of automated contracts (smart contracts) between the parties involved with definition of the type and manner of permitted use and linking the transfer of data to the fulfilment of the contract. SYNERGIES Smart Contracts manages and monitors compliance with the legally binding contract between data assets provider and consumers and only allows data transfer if all factors of the contract are met. Furthermore, smart contract mechanism will also prevent users accessing low quality or outdated data as part of IPR protection in case of fraudulent intent to use it.
3.	Technical security systems for transmission and storage	Tasks T3.3 and T7.1 deal with technical measures to secure transmission, storage and access such as Privacy Preservation Service, Encryption Engine, KeyTray or Security, Authentication & Authorisation Engine.
4.	Protection through monitoring of data quality and transmissions, corresponding alarm mechanisms and certification for trusted data sources	The Data Interoperability and Governance Block component, Data Observability Service, will monitor the data connections / data flow and triggers appropriate alarms whereas another component, Data Certification Service, ensures that data originates from a trusted right holder.
5.	Protection through encryption of data	Another protection option is to encrypt the data itself during its transmission and use.

Table 8: IPR Protection Measures

During the design of the SYNERGIES Energy Services Marketplace and the SYNERGIES AI Analytics On-Demand Service Platform, terms and conditions of access to platforms and the services will be put in place. Each user will be required to approved and agree on these terms and conditions before signing up for the platforms. Templates will be provided in the follow-up deliverables under Task T2.4 "Architecture Design and Technical Specifications". That's being said, another organisational measure indicated in the table above, data sharing contracts will be explained in the following section.

7.2.2 SYNERGIES Data Sharing Contracts

A data sharing contract is a formal legally binding agreement that licenses data exchange between two or more parties. It clearly documents what is being shared, for how long, how the data can be reused and other terms and conditions under which data can be re-used. Since ownership in data in legal sense as property ownership is not recognised neither by EU legislation nor by major European jurisdictions, data can only be licensed but not sold and both parties continue to have rights and responsibilities for the data. Therefore, a central role of a data sharing agreement is to clarify the allocation of benefits and risks and defines those rights and responsibilities of parties concerned. Such an agreement serves also further two purposes. First, it protects the right holder providing the data, ensuring that the data will not be misused. Second, it prevents miscommunication on the right holder over the data and the party receiving the data by making certain that any questions about data use are discussed.

In SYNERGIES Energy Data Space, data sharing contracts provide a common set of rules that, once approved, constitute a legally binding agreement for all stakeholders involved in the data sharing.



Therefore, before any data are shared, both the data assets provider and data assets consumers talk to discuss data-sharing and data-use issues and come to a collaborative understanding that will then be documented in a data-sharing contract. This contract and the agreed data sharing mechanism will be further automatically enforced by smart contracts through the implementation of the Smart Contract Management Engine. Therefore, smart contract will be programmed and configured based on the terms and conditions agreed under the data sharing contracts. As described in Task T3.4, SYNERGIES will provide a common set of terms and conditions for data sharing between data assets owner, data asset provider and data asset consumers under SYNERGIES Data Sharing Contract which will act as legal and give legitimacy to smart contracts.



Figure 8: The Envisaged Role of Data Sharing Contracts Between the SYNERGIES Stakeholders

For the data to be exchanged and utilised in the project, templates for data sharing contracts will be developed. In the process of implementing a data sharing contract, particular attention will be given to the following issues:

- 1. Clarify the type and categories of data such as personal data, sensitive data etc.
- 2. Understanding data sharing aims (purpose) and data quality requirements for the data being requested
- 3. Determine if the data is already available
- 4. Outline the benefits of sharing the data for the defined purpose, and decide if the benefits outweigh the costs of sharing
- 5. Verify the data assets providers or owners can share the data both in a legal and actual meaning
- 6. Identify data flow and data life cycle
- 7. Identify the entities and their personas in the data supply chain that control and process the data, and designate their respective roles in processing of personal data
- Identify the individuals whose data will be collected 8.

Given the intertwined and hyper connected nature of SYNERGIES Energy Data Space, the data sharing contracts focuses on multi-stakeholders, multiparty-ecosystem engagements and ensure that the stakeholders are committed to provide appropriate level of protection of IPRs.

Furthermore, due to risk of processing of personal data through data exchange in SYNERGIES Energy Data Space and other SYNERGIES data-driven activities, the SYNERGIES Data Sharing Contract will need to comply with the GDPR. Therefore, the contract will include additional provisions addressing i) what are the roles of the parties in the processing of personal data such as controller, processor or joint controller; ii) what is the purpose of data sharing; iii) what is the lawful basis for sharing according to



the GDPR; iv) whether or not data will be transferred to a country outside of EEA and on which legal grounds other organisations will be involved in the data sharing; v) What data items are going to be shared; vi) Is there any special category data, sensitive data or criminal offence data; vi) How will data subject rights be granted and enforced. Such additional provisions will help all data assets provider and consumers to justify data sharing and demonstrate that they have been mindful of, and have documented, the relevant compliance issues. Such data sharing contract provides a framework to help all stakeholders to meet the requirements of the data protection principles including accountability, transparency etc.

According to Task T3.4 "Trusted Data Sharing Block", the follow-up deliverable D3.1 "Energy Data Space Release 1.00" will provide the templates of SYNERGIES Data Sharing Contracts which will include all necessary instruments to legally bind the stakeholders involved in data sharing and to safeguard the integrity and enforcement of smart contracts.



Conclusions and Next Steps 8

This document, deliverable D1.1 – Project management plan, is fully aligned with the Grant and Consortium Agreements of SYNERGIES. It details the project management approach and structure, including the roles and responsibilities of governance bodies as well as all beneficiaries and members of the Project Consortium. It describes the structures, tools, processes, and procedures that WP1 (Project management) has instituted to ensure that the Project runs smoothly and effectively and in accordance with the Grant Agreement and contractual obligations.

Minor changes to structures and procedures might occur throughout the project lifetime, as a result of the continuous monitoring of activities and processes. However, the core of the Deliverable remains valid throughout the project duration.

The continuous monitoring will also be related to risk assessment and management and ethics. Moreover, updates about IPR, will take place at month 20 and 42, in correlation with task T6.3 "Exploitation strategy definition and Business Innovation Planning".



References

A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Online: https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

Al4People, Floridi, Luciano, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, Christoph Luetge et al.. White Paper, AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, 2018.

Audrey J. Dorofee, Julie A. Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy and Ray C. Williams, Continuous Risk Management Guidebook, Software Engineering Institute of Carnegie Melon University. Online: http://jodypaul.com/SWE/ContinuousRiskManagement.pdf

Court of Justice of the European Union, case SAS Institute C-406/10

Deliverable report of Ethics by Design and Ethics of Use in AI and Robotics published by the EU-funded SIENNA project in 2020.DESCA for Horizon Europe model CA version 1.0, July 2022. Available at https://www.desca-agreement.eu/desca-model-consortium-agreement/

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111/16. Available at https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A32009L0024.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 077/20 amended by Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130/70 (Database Directive).

European Commission IP Helpdesk, services provided. Available at https://intellectual-propertyhelpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk en

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Making the most of the EU's innovative potential, COM(2020) 760 final, available at https://eurlex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760#footnoteref2

European Commission, Directorate-General for Communications Networks, Content and Technology, Ethics guidelines for trustworthy AI, Publications Office, 2019, https://data.europa.eu/doi/10.2759/346720.

European Commission, Ethics by Design and Ethics of Use Approaches for Artificial Intelligence, Version 1.0, November 2021.

European Commission, EU Grants AGA – Annotated Model Grant Agreement, 20 November 2021.

European Commission, proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts, https://eur-lex.europa.eu/legal-COM/2021/206, available at content/EN/TXT/?uri=celex%3A52021PC0206.



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, available at <u>https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN</u>.

European Parliament, Intellectual, Fact Sheet on Industrial And Commercial Property, 2022 available at https://www.europarl.europa.eu/factsheets/en/sheet/36/intellectual-industrial-and-commercial-property#:~:text=Intellectual%20property%20includes%20all%20exclusive,includes%20artistic%20and%20literary%20property.

European Patent Office, Guidelines for Examination, Part G Patentability, March 2022.

European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019. Available at <u>https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai</u>.

Horizon IP Scan, services provided. Available at <u>https://intellectual-property-helpdesk.ec.europa.eu/horizon-ip-scan_en</u>

ISO 31000 – Risk management. Online: https://www.iso.org/iso-31000-risk-management.html

Organisation for Economic Co-operation and Development, Recommendation Of The Council On Artificial Intelligence, LEGAL/0449, 22 May 2019. Available at <u>https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#dates</u>.

Pasa, Barbara, Copyright and Data Protection, In book: Privacy and Data Protection in Software Services (pp.111-123), January 2022.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation) OJ L 119, available at: <u>https://eur-lex.europa.eu/eli/reg/2016/679/oj.</u>

Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013, OJ L 170/1, available at https://eur-lex.europa.eu/eli/reg/2021/695/oj

SYNERGIES, Consortium Agreement, 9 March 2022.

SYNERGIES, Grant Agreement No 101069839, 31 March 2022.

Zuiderveen Borgesius, Frederick, Study on discrimination, artificial intelligence and algorithmic decision-making, Council of Europe, 2018 referring to Barocas, Solon and Selbst, Andrew D, Big Data's Disparate Impact, 2016, SSRN Electronic Journal



Annexes

The templates related to project management tasks are included as annexes to the present document.

Annex I: Project management templates

Meeting Minutes including Agenda, Action list, Attendance list and Signature list



This project has received funding from the European Union's Horizon Innovation Actions - Sustainable, secure and competitive energy supply CL-5-2021-03-01 under Grant Agreement: 101059839



Shaping consumer-inclusive data pathwaYs towards the eNERGy transition, through a reference Energy data Space implementation

Minutes of Meeting

Meeting:

Location:

Date: XX/XX/202X

Dissemination Level: Version:

> Disclaimer. The views represented in this document only reflect the views of the authors and not the views of the European Union. The European Union is not liable for any use that may be made of the information contained in this document. Furthermore, the information is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user of the information uses it at its sole risk and Rabifity.



Agenda

Start*	duration	Торіс	Presenter	WP	Notes

Attendance List

No	Attendee	Partner
1		
2		
3		
4		
5		
6		
7		
8		

Action List

N o	W P	Action	Deadline	Owner	Status

Signature list



Meeting Information					
Date:					
Location:					
Purpose:					

Signatures

Name and Surname	Company	Signature



PPT Presentation Template

V STREKOL
141
🔅 SYNERGIE
an
IES
DD/MM/YYY Name & Surname



Table of Contents	💱 SYNERGIE
Click to edit Master text styles	
	(4)
	SYNERGI
WP##	
Edit <u>title</u>	
Click to add subtitle	
Click to add title	💱 SYNERGI
Click to edit Master text styles	Click to edit Master text styles
 Click to edit Master text styles 	Click to edit Master text styles
Second level Third level	Second level Third level
Fourth level	Fourth level
Hifth lével 🧐	Fifth level 🧐







Deliverable Template



This project has received funding from the European Union's Horizon Innovation Actions - Sustainable, secure and competitive energy supply CL-S-2021-D3-01 under Grant Agreement: 101069839



Shaping consumer-inclusive data pathways towards the eNERGy transition, through a reference Energy data Space implementation

WPX: WP Title

DX.X: Deliverable Title

Deliverable Leader: XXXX Due Date: MXX Dissemination Level: XXXX Version: XXX

Disclaimer. The views represented in this document only reflect the views of the authors and not the views of the European Union. The European Union is not liable for any use that may be made of the information contained in this document. Furthermore, the information is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user of the information uses it at its sale risk and linhility.



Contact and Mailing List

	в	С	D	E	G	н	1	J	к
1	ID	Partner	Name Surname	email	SYNERGIES Role	main mailing list/portal access	ML: administrative	ML: technical	ML: demonstrators
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									