This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 953016

SERENDI PV

D7.3 Assessment and recommendations on legal aspects, policy, confidentiality, data privacy

T7.3 Assessment of legal aspects, policy, confidentiality, data privacy

Grant Agreement nº:	**953016**
Call:	H2020-LC-SC3-2020-RES-IA-CSA / LC-SC3-RES-33-2020
Project title:	**Smooth, REliable aNd Dispatchable Integration of PV in EU Grids**
Project acronym:	SERENDI-PV
Type of Action:	Innovation Action
Granted by:	Innovation and Networks Executive Agency (INEA)
Project coordinator:	Fundación TECNALIA Research & Innovation
Project website address:	*www.serendi-pv.eu; www.serendipv.eu*
Start date of the project:	October 2020
Duration:	48 months

Document Ref.:	SERENDI-PV-D7.3_Assessment and recommendations on legal aspects, policy, confidentiality, data privacy_V1.docx
Lead Beneficiary:	Becquerel Institute
Doc. Dissemination Level:	**PU**– Public
Due Date for Deliverable:	30/03/2022 (M18)
Actual Submission date:	30/04/2022 (M19)
Version	V1

Summary

This report deals with legal aspects, policy, confidentiality and data privacy for data linked to PV power generation, focusing on grid connected systems. First, it provides an inventory of relevant definitions for data, data types, data agreement types, and legal instruments for data governance. In the practical implementation section: guidelines and models for data sharing are presented. Then recommendations about data management of liabilities for PV power generation related data is presented. Finally, further recommended literature is included in the report.

Document Information

Title	Assessment and recommendations on legal aspects, policy, confidentiality, data privacy
Lead Beneficiary	Becquerel Institute
Contributors	MLS, NKW, SolarGIS, QPV, Lucisun
Distribution	Public
Report Name	Assessment and recommendations on legal aspects, policy, confidentiality, data privacy

Document History

Date	Version	Prepared by	Organisation	Approved by	Notes
03/02/2022	V0.1	Monica Aleman, Gaëtan Masson Joseph Reed, Nada Suriova, Tatiana Ziakova Elias de Keyzer	BI MLS Solargis S.R.O. NKW		
06/04/2022	V0.2	M. Aleman I. Lombardero	BI QPV		
27/04/2022	V1.0	J. del Pozo	TECNALIA		Submitted to the EC

Acknowledgements

The work described in this publication has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 953016.

Disclaimer

This document reflects only the authors' view and not those of the European Commission. This work may rely on data from sources external to the members of the SERENDI-PV project Consortium. Members of the Consortium do not accept liability for loss or damage suffered by any third party as a result of errors or inaccuracies in such data. The information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and neither the European Commission nor any member of the SERENDI-PV Consortium is liable for any use that may be made of the information.

Contents

Tables

Figures

1 EXECUTIVE SUMMARY

1.1 Description of the deliverable content and purpose

This report has been prepared as part of the SERENDI-PV project by the Becquerel Institute with the contribution in the drafting of the following project partners: MyLight Systems, SolarGIS, Lucisun, Next KraftWerke and QPV.

The target of this report is to provide on one hand background information about data sharing and data governance to then present an inventory of legal aspects related to data distribution and use of software tools relevant for the sharing of data in the PV sector. It serves as an input for the collaborative platform created during the SERENDI-PV project.

The report is structured as follows:

- First an introduction into the main terms implemented in a data management framework, both from a legal and a technical perspective, including the definition of the different types of data and data agreements is presented. This is followed by a general overview of the legal instruments for data governance in the EU.
- A practical implementation section provides an overview of the current data flows around the PV sector, presenting the both the main stakeholders working with data in the PV sector around the PV plant and the data they potentially exchange with the other stakeholders. Guidelines for the creation of data sharing agreements and models for data sharing are presented.
- This is followed by a list of recommendations for the management of liabilities and penalties linked to data flows in the PV sector.
- Finally, a non-exhaustive list of further recommended literature and relevant content for data sharing in the energy sector is displayed.

The information presented in this report has been gathered by a combination of desk research, interviews with project partners (Akuo, CNR, Cobra) and completed with the experience of the drafting partners.

1.2 Relation with other activities in the project

Table 1.1 depicts the main links of this deliverable to other activities (work packages, tasks, deliverables, etc.) within SERENDI-PV project. The table should be considered along with the current document for further understanding of the deliverable contents and purpose.

Table 1.1: Relation between current deliverable and other activities in the project

Project activity	Relation with current deliverable
1.4	Deals with specifications on data collection, database, transfer protocols, data privacy and distribution and IP: in this task the data needs, formats and best storage and sharing methods are investigated
6.2	Defines databases and data flows exchanges with system operators, regulatory agencies and environmental and governmental authorities
7.1	Creation of a web-based common collaborative platform environment: the inventory of legal aspects reported in this document will support the implementation of innovative solutions featured in the collaborative platform.
7.2	Development of common data collection, QC and filtering, database and transfer protocols, standardization and interoperability: the inventory of legal aspects reported in this document could be useful for T7.2
10.3	Data Management Plan: identification of the data types implemented in the SERENDI-PV project.
11.2	D11.2: POPD - Requirement No. 2 [M6] 4.2 The host institution must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be submitted as a deliverable. 4.13 In case the research involves profiling, the beneficiary must provide explanation how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded. This must be submitted as a deliverable.

1.3 Abbreviation list

Table 1.2: Abbreviations table

	Meaning
ACER	Agency for the cooperation of energy regulators
AI	Artificial Intelligence
API	Application Programme Interface
BRP	Balancing Responsible Party
DPA	Data Processing Agreement
DSO	Distribution Systems Operator
EE	Energy Efficiency
EMD	Electricity Market Directive
Entso-E	European Network of Transmission System Operators for Electricity
EULA	End User Licence agreements
FDD	Fault Detection and Diagnostics
GDPR	General Data Protection Regulation
ML	Machine Learning
NDA	Non-disclosure agreement
O&M	Operations and Maintenance
PV	Photovoltaic
REDII	Renewable Energy Directive II
RES	Renewable Energy Sources
SaaS	Software as a Service
SLA	Service Level agreements
T&C	Terms and Conditions
TFEU	Treaty on the Functioning of the European Union
ToS	Terms of Service
ToU	Terms of Use
TSO	Transmission Systems Operator
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

2 INTRODUCTION

The EU is currently defining strategies for the creation of a **data economy.** In a modernized digital energy system, all infrastructure and assets will be described by data, monitoring and analytics will work together to provide a detailed view of the system state over time and data will be used to optimise operation and drive markets [1]. The data strategy aims to play a key role in the digital transformation developing strategies such as the free flow of non-personal data regulation, the European database directive, (see 2.4).

The existence of a sound legal framework for the transparent and secure collection, processing and dissemination of data and software tools becomes increasingly important. The aim of this report is to gather the most important concepts and legislation currently available for the data governance in the PV sector, particularly when linked to PV generation, considering legislative concepts and measures in a context where the data generation is moving from single data points to big data analytics.

This information will serve as an input for the collaborative platform developed in the SERENDI-PV project.

2.1 General Definitions

The following table introduces general concepts relevant in the data creation, management and utilisation.

Table 2.1: General definitions and relevant concepts linked to data management in PV

Data management	
Data governance	Policies and procedures implemented to ensure an organization's data is accurate and handled properly. Includes a description of the data model (describing data flows), and the governance model overlaying the rules, activities, responsibilities and protocols. [2]
Dataspaces [3]	Approach to data management, where data is integrated on an "as needed" basis, with labour intensive aspects of data-integration postponed until they are required. The EC is defining a strategy to create common dataspaces for strategic sectors, aiming to overcome legal and technical barriers for data sharing [4]
Interoperability	Functional interconnection and interaction, providing the ability to exchange information and to mutually use information which has been exchanged.
Data sharing	Means allowing third parties specifically permissioned access to datasets to generate value [5]

Data analysis	
AI datasets	Artificial Intelligence (AI) is any technique which enables computers to mimic human behaviour, such as decision-making algorithms, statistical models, search of methods and optimization theory, game theory
Machine Learning (ML)	It is a subset of AI including statistical techniques enabling machines to improve at tasks with experience. It can be supervised or unsupervised.
Deep Learning (or deep neural learning)	It is a subset of machine learning, using the neural networks to analyse different factors. Multi-layered models that learned representation of data with different levels of abstraction
Digital Twin	Virtual replica (model) designed to accurately reflect the physical world (object, process, or service), spanning its lifecycle. It provides a digital representation (i.e simulation model, data-driven model) that updates and changes as the physical twin changes. It is constructed from multiple sources of data (real-time, historical, sensor data), and it uses simulation, machine learning and reasoning to help decision making. It enables the prediction of how a product or process will perform, e.g. a machine failure could be avoided thanks to the implementation of predictive maintenance

Basic concepts	
Anonymization	Techniques for lowering the risk of identification of data subjects from data, typically done by removing or aggregating data which could help identify data subjects combined with other measures such as adding noise [5]
APIs	Application Programming Interfaces, small software services that can be used to open up data or services within a software package, including in the cloud.
Primary data	It is the raw information and/or knowledge, which can be generated, collected, assembled, measured, communicated.
Metadata	Data about data: Data that provides information about other data. It can be a service or account data derived from the use of a service by a customer. It is not the input of the customer but the service. Includes: Date and time of creation, source, size and data quality. It can be the raw material for AI/ML/DL - its creation use and ownership are subject of negotiation
Derived data	(Second or subsequent generation) Data that is created or derived from (first generation) data. Creating it may involve use of first-generation data in a way that infringes the rights of first-generation data owner, requiring permission or license.
Linked data	Method by which structured data can be published, looked up via HTTP; queried and linked to other data by computers. It provides an URL (uniform resource locator). Data can be identified by an URI (Uniform Resource Identifier). It can be proceeded in a format that can be accessed, queried, and linked to other data by computers
Pre-processed data	It involves the preparation and validation of the data, for example cleaning, selection, re-sampling, normalization, transformation, feature extraction and selection of data. It may also involve the creation of metadata. [6]
Big data	Relates to the aggregation, analysis and value of exploitable datasets (structured and unstructured data)

Other relevant concepts for data in the PV sector include data readiness (maturity), and the consideration of the different platforms to organize data protocols.

2.2 Data types

Table 2.2 lists various options for data classification relevant in the PV sector depending on the structure, confidentiality, time frame, and nature of the data

Table 2.2: Data classification options

Classified by		Definition
Structure	**Data vs Database**	**Data** is the primary data, not treated or manipulated in any way. Sometimes mentioned as a digital object. **A database** can be considered as structured data. It is the system where the information is collected.
	Structured vs Unstructured data	**Structured data** is formatted and organized in a pre-defined way so that processing and analysis can be applied. **Unstructured data** is not organised or defined before being sent.
Confidentiality	**Confidential vs Public data**	**Confidential data** refers to personal information which is shared in confidence with another party. Confidentiality agreements are often implicit. **Private** data may be read by the users with access to that data library, while **public data** is accessible by all users.
	Pseudonymized vs Anonymized data	**Anonymization**: when it is not possible to restore the original information. **Pseudonymization** replaces sensitive data, subject can still be identified through indirect or additional information
Time frame	**Real-time, Delayed and Reference data**	**Real-time** (chargeable) data is delivered virtually instantly with its creation. **Delayed data** (non-chargeable) varies between data providers. **Reference data** includes historical or non-real time information.
Nature of the data	**Personal** vs **non personal** **Financial** – e.g. CAPEX, OPEX, loans… **Technical** data – e.g. PV production, weather forecast, data availability **Time series** data- e.g; spot price, generation or outage time series **Geospacial** data **Environmental** e.g. impact on biodiversity **Legal** – e.g. data required for permitting	

2.3 Data agreement types

Data agreements determine the purpose of data sharing, including defining the use of data at each stage, setting standards, and helping define the roles and responsibilities regarding the data for all the parties involved. Different types of agreements can be made depending on the data and the purpose of use between the stakeholders. Table 2.3 presents the features and provisions for the main type of agreements relevant for data and software.

Table 2.3: Main features and provisions for data and software agreements

Type of agreement	Description	Provisions
Data sharing agreement	Formal contract clearly documenting data being shared and its uses. It protects the agency providing the data, ensuring that the data will not be misused, and it prevents miscommunication on the part of the provider of the data and the agency receiving the data. Before any data is shared, both: provider and receiver discuss data-sharing and data-use issues and come to a collaborative understanding, documented in a data-sharing agreement.	• Period of agreement • Intended use of the data • Constraints on use of the data • Confidentiality • Security • Methods for data sharing • Financial costs for data sharing
License agreements. Such as End User Licence agreements (EULA) [7]	Legal contracts between two parties: an owner (licensor) and a second party (licensee). The owner gives official permission to the licensee to do, use or own something (a software, a brand, a patented technology, or the ability to produce and sell goods) by the licensor. So, a licence agreement grants the licensee the ability to use the IP owned by the licensor. They are commonly used to commercialize IP.	• Nature of the agreement, • Copyright or IP right: clarifying ownership • Limitation of liability clauses • Disclaimers • Governing Law • Right to terminate the agreement • Authorized use • Unauthorized use Other aspects to consider are: Third parties, right to modifications, right to sell.
Terms of Use / ToU, Terms and Conditions T&C, Terms of Service ToS, User Agreements, Terms of User Agreements, acceptable Use Policy	These are legally binding agreements between a **service provider** and a person who wants to use that service. The person must agree to abide by the terms of service in order to use the offered service. [1] Terms of service can also be merely a disclaimer, especially regarding the use of websites. Vague language and lengthy sentences used in the terms of use have brought concerns on customer privacy and raised public awareness in many ways.	• Governing law: jurisdiction • Disclaimers • Liability limitation • Rules of Account Termination • Permitted and Restricted Use (including user behaviour/guidelines) • How to register for an Account • Need to specify a right to terminate the owner's services to a specify user and not just the license of the software.
Non-Disclosure Agreements (NDAs)	Legally binding contract establishing a confidential relationship between the parties involved, to protect information required to do business.	• Parties involved • Definition of confidential information • Disclosure period • Authorized use, • Terms for disclosure • Exclusions • Legal provisions • ToU, or T&C • Law governing the parties

Other types of data sharing agreements include the Standard Software License sharing agreements and Service Level agreements (SLA).

2.4 Legal instruments and measures for data governance in the EU

The EU has several legal instruments affecting data sharing. The most relevant for the management of data in the PV sector (also including some considerations for the electricity generation) are listed in Table 2.4. This list presents general information linked to data sharing from the legislation, as well as its purpose.

A deeper assessment of the regulations, legislations and measures impact of on the data governance for PV data flows is presented in chapter 4, Section 4.3: Particularly focusing to liabilities and penalties.

Table 2.4: EU's relevant cross-sectoral legislations and measures relevant for data governance in the PV sector

Instrument	Year	Information	Objective [8]
GDPR: General Data Protection Regulation [9]	2016 Applicable since 2018	Defines rules applicable for personal data for EU and EU residents	Protect fundamental rights and freedom of natural persons and their right to protection of personal data
TFEU: Competition law – Treaty on the Functioning of the European Union [10]		Requires sharing of information which could enable market access to third parties. When defining licensing agreements, a company muss assess whether it runs afoul of the constraints imposed by article 101 [8]. data making third parties; Article 102 requires data sharing practices conductive to competition to avoid abuse of position of power. The act of making innovation impossible by refusing to make data available to third parties can be as such ground for intervention at least in some instances. A consequence from the application of article 102 can be a proactive data interoperability policy	Mainly via articles 101 and 102: It aims to ensure that fair competition is not distorted in the internal market and that the open market economy is protected. This is particularly interesting when considering new market entrants such as aggregators, flexibility providers, and prosumers

Instrument	Year	Information	Objective [8]
Database directive [11]	96/9/EC	Defines statutory framework for legal protection of structured data in EU. It defines two types of IPR. 1) **copyright** (if "by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation. (2) **Sui generis right**, applying to databases "which show that there has been qualitatively and/or quantitative a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively of the contents of that database (7.1)	Harmonizing requirements for database protection by applying higher standards (creativity) and lower standards (investment required for making the database) depending on the nature of the database. Without a certain threshold of originality databases do not attract copyrights [12]
Directive on copyright in the digital single market [13]	Directive (EU) 2019/790	Foresees more exceptions in relation to copyright and sui generis for databases, including text and data mining for scientific purposes,	Ensure fairer remuneration for creators and rightsholders when the work is used online. Defining who is legitimately able to share content
Free flow regulation of non -personal data in the EU [14]	Regulation 2018/1807	It creates codes of conduct for example for cloud providers with Software as a Service (SaaS) and infrastructure as a service (IaaS)	Remove barriers to the free flow of non -personal data in the internal market
The software directive [15]	2009/24/EC of the EP and the council	Legal protection of computer programs sets rules to protect computer programs as literary works under copyright law. Article 6 requires decompilation without the authorisation of the rightholder under specific conditions; incentivises data sharing of the information required to enable interoperability. When software operates remotely as a service, a user has no practical option to decompile it. The emphasis of the market has shifted towards APIs (check reworking of the PSI directive)	Protect computer programs under copyright law, as literary works. Including the right to reproduction, translation, adaptation, alternation and distribution of the computer program; mirrored by restricted acts.
Standards: ISO 38505 (data governance) [16]	ISO/IEC 38505:2017	Looks at the governance of data and its use within an organization,	Provide guidance for current and future use of data that is created, stored or controlled by IT systems
Transparency regulation [17]	543/2013/EC	Requires TSOs and market actors to publish a wide range of detailed specific market data through the ENTSO-E platform	Serve market participants, particularly SMEs, making data available to market participants and to the public in an easy, accessible, downloadable and free of charge way.

Instrument	Year	Information	Objective [8]
REMIT: Regulation on Wholesale Energy Market Integrity and Transparency [18]	1348/2014/ EC	Article 4: Market participants publicly disclose in and effective and timely manner inside information they possess	Increase transparency and stability of EU energy markets while combating insider trading and market manipulation
Data Act: Proposal for a regulation EU Data Governance [19]	COM/2020/767	Make public sector data available for re-use, sharing data among businesses (against remuneration), allowing personal data to be used with an intermediary, enabling the protection of rights under the GDPR, allowing data use on altruistic grounds	Forster the availability of data for use by increasing trust in intermediaries and strengthening data sharing mechanisms across the EU
FAIR data guidelines, go Fair initiative [20]	2016 	Currently being requested in R&D project, FAIR guidelines aim to improve the **F**indability, **A**ffordability, **I**nteroperability and **R**euse of digital assets. Typically considers domain-relevant metadata exchanges	Provide information in a way that it emphasises machine actionability. It aims to optimize the reuse of data

3 PRACTICAL IMPLEMENTATION

This section focuses on data flows for grid connected PV plants acting as legal entities.

3.1 Models for data sharing

Models for sharing data are strongly dependent on the type of data, the sensitivity of the data and the technological level of the organization.

I. Open data licenses

An Open Data approach, the data is made available by the data supplier to an (in principle) open range of (re-)users with as few restrictions as possible and against either no or very limited remuneration, can be chosen when the data supplier has a strong interest in the data re-use. Examples are providers of services that would like to make use of an ecosystem of third-party application developers in order to reach the final customers. There are public domain dedications, attribution licenses and share-alike licenses [12].

II. Creative commons license

There are 6 different license types. It allows reusers to distribute, remix, adapt and build upon material in any medium or format as long as attribution is given to the creator. It allows for commercial use. It allows the copyright owner to define what (re)users can and can't do with their work.

Creative Commons licences

Licence	Symbol	Description
Attribution		It can be copied, modified, distributed, displayed and performed but the copyright owner must be given credit.
Non-commercial		It can be copied, modified, distributed and displayed but no profit can be made from it.
No Derivative Works		It can be copied, distributed, displayed and performed but cannot be modified.
Share-alike		It can be modified and distributed but must be covered by an identical license.

Figure 3.1: Symbolic description of the 4 most used Creative commons licenses [21]

III. Data monetisation on a data marketplace

Data monetisation or trading can take place through a data marketplace as an intermediary based on bilateral contracts against remuneration. It can be interesting for companies that do not know potential re-users for their data and aim at engaging in one-off data monetisation efforts. This mechanism appears suitable when either (1) there are limited risks of illicit use of the data in question, (2) the data supplier has grounds to trusts the (re-)user, or (3) the data supplier has technical mechanisms to prevent or identify illicit use. Model contract terms can lower the costs of drawing up data usage agreements.

IV. Data exchange in closed platform

Data exchange may take place in a closed platform, either set up by one core player in a data sharing environment or by an independent intermediary. The data in this case may be supplied against monetary remuneration or against added-value services, provided e.g. inside the platform. This solution allows offering added-value services and thus provides for a more comprehensive solution for more stable data partnerships and allows for more mechanisms of control on the usage made of the data; model contract terms can lower the costs of drawing up data usage agreements. Where the data sharing is exclusive, it would need to comply with the competition rules.

V. EU B2B data sharing

B2B data sharing involves the following principles:

a) Transparency: The relevant contractual agreements should identify in a transparent and understandable manner (i) the persons or entities that will have access to the data that the product or service generates, the type of such data, and at which level of detail; and (ii) the purposes for using such data.

b) Shared value creation: The relevant contractual agreements should recognise that, where data is generated as a by-product of using a product or service, several parties have contributed to creating the data.

c) Respect for each other's commercial interests: The relevant contractual agreements should address the need to protect both the commercial interests and secrets of data holders and data users.

d) Ensure undistorted competition: The relevant contractual agreements should address the need to ensure undistorted competition when exchanging commercially sensitive data.

e) Minimised data lock-in: Companies offering a product or service that generates data as a by-product should allow and enable data portability as much as possible [8]. They should also consider, where possible and in line with the characteristics of the market they operate on, offering the same product or service without or with data.

VI. Private data sharing

With regards to private data and GDPR, the following provisions must be considered:

- The processor agrees to process personal data only on written instructions of the controller.
- Everyone who comes in contact with the data is sworn to confidentiality.
- All appropriate technical and organizational measures are used to protect the security of the data.
- The processor will not subcontract to another processor unless instructed to do so in writing by the controller, in which case another DPA will need to be signed with the sub-processor (pursuant to Sections 2 and 4 of Article 28).
- The processor will help the controller uphold their obligations under the GDPR, particularly concerning data subjects' rights.
- The processor will help the controller maintain GDPR compliance with regard to Article 32 (security of processing) and Article 36 (consulting with the data protection authority before undertaking high-risk processing).
- The processor agrees to delete all personal data upon the termination of services or return the data to the controller.
- The processor must allow the controller to conduct an audit and will provide whatever information necessary to prove compliance.

3.2 Stakeholder and data flows identification

A relevant step when considering legal practices for data sharing is the identification of the stakeholders. In this section we identified the main stakeholders involved in the data flows and the type of data they exchange. The result of this evaluation is depicted Figure 3.2 for grid-connected PV systems.

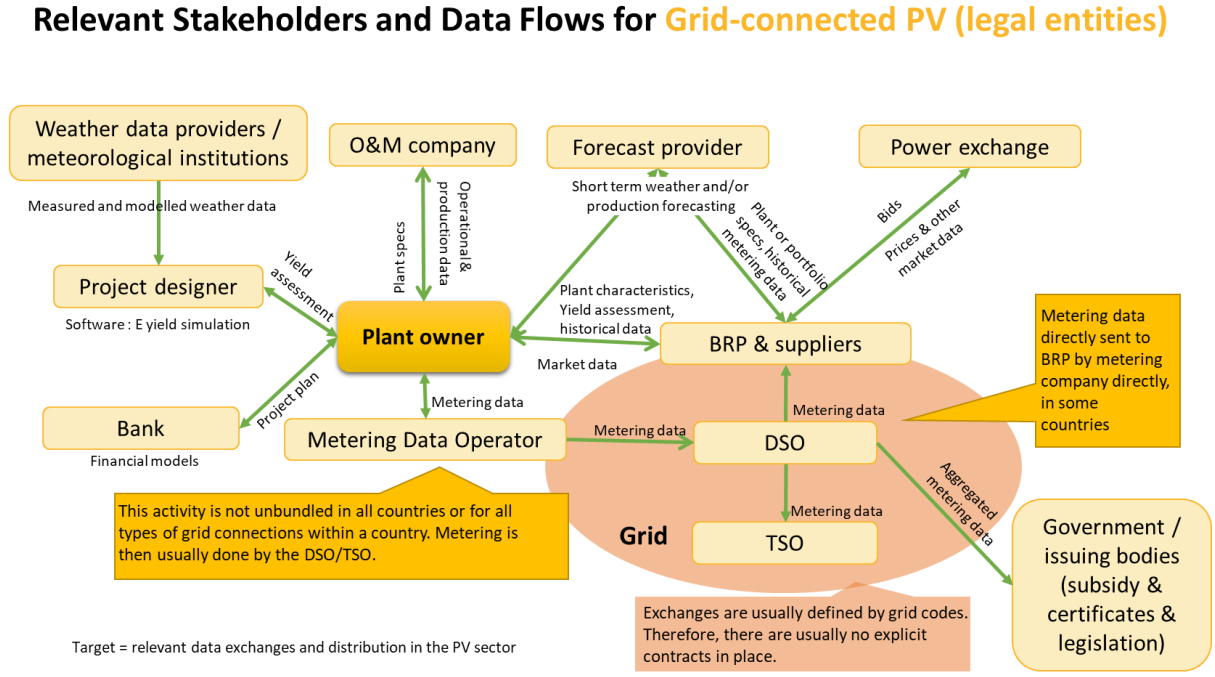

Figure 3.2: Main Stakeholders and Data Flows for Grid-connected PV systems (as legal entities)

The stakeholder view has been simplified to present it depending on the type of relation with the project owner (see Figure 3.3). Four "standard" relationships to the project owner have been selected, so that we can quality stakeholders other than the PV owner as : (I) commercial partners, (II) Regulators / Governmental authorities, (III) Financial institutions, (IV) PV Energy Management/ trading.

The stakeholders identified as commercial partners or service suppliers are companies providing (1) Operations and Maintenance (O&M), (2) Asset managers, (3) Forecasting data providers, (4) Monitoring data providers, (5) Consultancies. As regulators or governmental authorities there are (5) regulatory bodies, (6) Distribution System Operators (DSO), (7) Transmission System Operators. As Financial institutions we have considered (8) Investors and funds, (9) Banks and financial institutions providing loans for PV projects, (10) Insurance companies. Finally, in the PV Energy management and trading there are (11) Flexibility providers and (12) Energy traders.

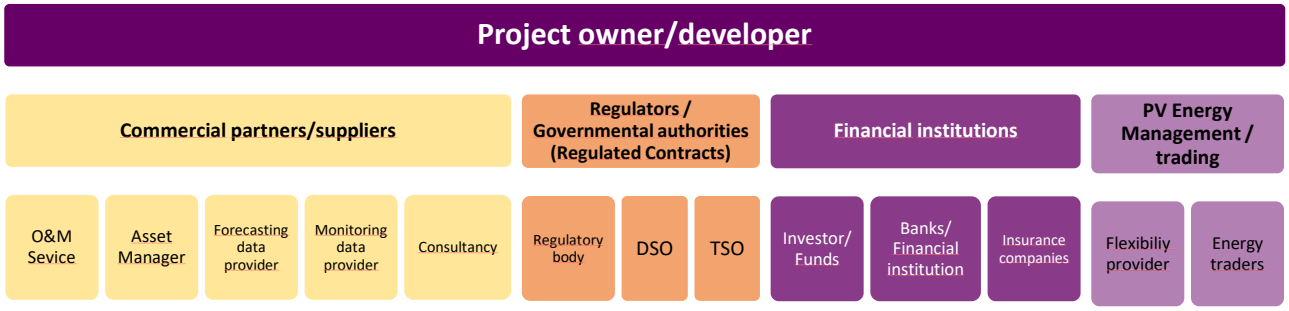

Figure 3.3: stakeholder classification based on the relation to the PV asset owner

The feedback from the developers involved in the project is that besides the regulated data flows: with governmental authorities, regulators or environmental agencies (see deliverable 6.1 of the SERENDI-PV project) , the type of agreements arranged with third parties, where data is involved, is not so strongly linked to the position of the stakeholder in a sector map, but to the sensitivity of the data to be shared. They also mentioned that most of the services where sensitive data is involved is performed by internal groups within the respective organisations.

3.3 General guidelines for data sharing agreements

Following provisions should be considered when drafting a data sharing agreement:

1. **Parties involved**
   - Who are the parties involved in the agreement?
2. **Purpose of the sharing initiative / intended use of the data**
   - What is the aim?
   - Why is sharing the data necessary to achieve those targets?
     - State as specifically as possible how the receiver will use the data.
     - What studies will be performed, what questions will be asked and what are the expected outcomes?
     - Can the receiver use the data to explore additional research questions without the approval or consent of the provider?
   - What are the benefits expected from the data sharing?
3. **Period of agreement:**
   - Clearly define when the provider will give the data to the receiver and how long the receiver will be able to use the data.
   - Once the receiver agency no longer has the right to use the data, what will happen?
   - Will the data be returned to the provider, or will it be destroyed (deleted from hard drives, shredded, burned, etc.)?
4. **Constraints on use of the data:**
   - List any restrictions on how the data or data findings can be used.
   - Is the receiver required to document how the data are used?
   - Can the receiver share, publish or disseminate data findings and reports without the approval or review of the provider?
   - If the receiver generates a report based on the data, does the report belong to the receiver or the provider?
   - Can the receiver share, sell or distribute data findings or any part of the database to another agency?
5. **Data confidentiality (when sensitive data is involved)**
   - Describe the required processes that the receiver must use to ensure that data remain confidential.
   - Because some data may contain information that can be linked to individuals, it is important to put safeguards in place to ensure that sensitive information (e.g., salaries, exam results) remains private.
   - Personal data should remain confidential and should not be disclosed verbally or in writing to an unauthorized third party, by accident or otherwise.
   - Will the receiver report information that identifies individuals?
   - What safeguards are in place to prevent sensitive information from becoming public?

6. **Data security**
   - Describe the methods that the receiver must use to maintain data security.
   - Hard copies of data should be kept in a locked cabinet or room and electronic copies of data should be password protected or kept on a secure disk.
   - Will everyone at the receiver agency have the same level of access to data, or will some people have restricted access?
   - What kind of password protections need to be put in place?
   - Who will have physical access to the data, including the servers and the paper files?
   - What will happen to the data after the data-sharing period ends?
7. **Methods of data-sharing**
   - Identify the way in which data will be transferred from the provider to the receiver.
   - How will the data be transferred?
   - If data is to be sent over the Internet, how will the connection security be guaranteed?
   - Will the data be encrypted before being transferred?
8. **Financial costs of data-sharing**
   - Clarify who will cover the monetary costs of sharing the data.
   - Will there be expenses related to sharing the data?
   - Will the provider or the receiver share the costs, or will one agency pay for all data-sharing expenses?

For a **FAIR data** series [22], the following guidelines have been extracted from the GO FAIR initiative

Table 3.1: FAIR guiding principles

Making data FINDABLE, including for provisions of metadata
• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how
Making data ACCESIBLE
• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions

Making data INTEROPERABLE
• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?
Making data REUSABLE
• Check that the description of the data is plural, • (Meta) Data is associated with a clear and accessible usage licence • (Meta) Data are associated with a detailed provenance • (Meta) Data meet(s) domain relevant community standards

4 RECOMMENDATIONS ABOUT MANAGEMENT OF LIABILITIES AND PENALTIES

NDAs and commercial contracts can be divided into two main groups:

I. Standard NDA and standard commercial contract between private and legal entities (governed by mutually agreed contractual documents)

II. Contracts (or NDAs) between private or legal entities and governmental authorities (legal documents regulated by specific national or EU legislation)

4.1 Commercial NDAs

Table 4.1: Most commonly used provisions of liabilities and penalties in commercial NDAs

STANDARD NDA (data exchange or data provision)	
Commercial entities included	*Private person included*
Liabilities	
• Applicable to confidentiality breach and misuse / improper handling of confidential material during and after the end of NDA validity • Liability for breach can be associated with the obligation to pay damages or to take other appropriate measures if enforced by the damaged party • NO liability for completeness and accuracy of the data provided under NDA • NO liability for any errors or omissions related to the data provided under NDA	• Handling of the personal data should be considered as in line with GDPR if it is for the contract purposes (personal data processing shall be lawful if processing is necessary for the performance of the NDA to which the private person is a party) • Separate processor contract does not need to be signed in the above cases • Protection of personal data should be however assured and maintained under both, GDPR as well as within the frame of confidentiality obligations based on NDA.
Penalties (if explicitly agreed in the NDA or applicable by law in case of GDPR)	
• Confidentiality breach / breach of NDA terms • Improper handling of confidential material during or after termination of the NDA • NO penalty for inaccurate data / incomplete data	• Improper handling of personal data - applicable in cases where protection of data was not assured pursuant to GDPR or there is a reason to take special measures under GDPR (like signing a data processing contract)

4.2 Contracts (NDAs) between private or legal entities and governmental authorities

Table 4.2: Most commonly used provisions of liabilities and penalties in commercial contracts

STANDARD COMMERCIAL CONTRACTS or DATA TERMS & CONDITIONS (data exchange or data provision)	
Commercial entities included Independent service providers, PV system owners or operators or asset managers, energy traders, private or commercial aggregators etc.	*Private person included* Private PV owner, communities of the owners (PV electricity producers or suppliers)
Liabilities	
• Late delivery • Data supply disruption • Missing / incomplete data • Breach of confidentiality • Breach of IP rights / data terms of use • NO liability for data accuracy • NO liability for results obtained by customer by using the data • Liability for breach can be associated with the obligation to pay damages or to take other appropriate measures if enforced by the damaged party	• Handling of personal data should be considered as in line with GDPR if it is for the contract purposes and a separate processor contract does not need to be signed in such cases (personal data processing shall be lawful if processing is necessary for the performance of a contract to which the private person is party, such lawful processing however does not exclude the obligation to protect the personal data provided within the contract) • It is possible that under certain conditions data processing contract must be signed (in case of 3rd party personal data are processed)
Penalties (if explicitly agreed in the contract or applicable by law in case of GDPR)	
• Breach of any (above mentioned) provision of the contract	• Breach of protection measures pursuant to GDPR and/or GDPR processor contracts (if applicable)

4.3 Responsibilities – liabilities and penalties identified in regulated contracts

EU legislation (adopted at the level of the of the European Parliament and of the Council) and relating national legislation, that might have implications on the regulation of data flow in the process of PV electricity production / consumption (national and international):

Directive (EU) 2019/944 on common rules for the internal market for electricity and amending Directive 2012/27/EU - EMD (Electricity market directive)

- It outlines rules for the generation, transmission, distribution, supply and storage of electricity, together with consumer protection aspects, aiming to create integrated competitive, consumer-centered, flexible, fair and transparent electricity markets in the EU
- Among other things, it contains rules on retail markets for electricity
- It aims at the completion of internal electricity market, promoting free access to the market and fair competition, facilitation of cross border access for new suppliers from different sources.

Regulation (EU) 2019/943 on the internal market for electricity

- Mainly contains rules for wholesale market and network operation
- Sets out a number of principles on which electricity markets should be operated including to encourage free price formation and avoid actions which prevent price formation on the basis of supply and demand, facilitate the progressive removal of obstacles to cross-border flows of electricity between bidding zones or EU countries and to cross-border transactions on electricity and related service markets

Directive (EU) 2018/2001 on the promotion of the use of energy from renewable sources (recast) - REDII (Renewable energy directive)

- Establishes a common framework for the promotion of energy from renewable sources
- It sets a binding Union target for the overall share of energy from renewable sources in the Union's gross final consumption of energy in 2030
- Lays down rules on financial support for electricity from renewable sources, on self-consumption of such electricity, on the use of energy from renewable sources in the heating and cooling sector and in the transport sector

REGULATION (EU) 2019/941 on risk-preparedness in the electricity sector

- Lays down rules for cooperation between Member States with a view to preventing, preparing for and managing electricity crises in a spirit of solidarity and transparency and in full regard for the requirements of a competitive internal market for electricity
- It is intended to contribute to the implementation of energy security, solidarity and trust

Regulation (EU) 2019/942 establishing a European Union Agency for the Cooperation of Energy Regulators (ACER)

- Establishes a European Union Agency for the Cooperation of Energy Regulators (ACER)
- ACER ensures that the integration of national energy markets is met according to the EU's energy policy objectives and regulatory frameworks
- Close cooperation with ENTSO-E

Table 4.3: Specific conditions of regulated contracts (linked to data governance the PV sector)

SPECIFIC CONDITIONS OF REGULATED CONTRACTS (Data provision or data exchange) For the purpose of connection to the electricity grid, supply of electricity/surplus to the grid, forecast data etc.		
Responsible party	**Description**	**Reference to EU law**
Responsibility - Liability		
Regulatory authority	Non-discriminatory access to customer consumption data, the provision, for optional use, of an easily understandable harmonised format at a national level for consumption data, and prompt access for all customers to such data pursuant to Articles 23 (Data management) and 24 (Interoperability requirements and procedures for access to data) of the Directive	Directive (EU) 2019/944
Member states	Ensure a level playing field where electricity undertakings are subject to transparent, proportionate and non-discriminatory rules, fees and treatment, with respect to balancing responsibility, access to wholesale markets, access to data, switching processes and billing regimes and, where applicable, licensing	
Energy traders (NEMO, TSO)	(Day ahead and intraday market) - To be transparent while at the same time protecting the confidentiality of commercially sensitive information and ensuring that trading occurs in an anonymous manner	Regulation (EU) 2019/943
Electricity undertakings	Apply the procedures so that competent authorities can have access to the data of the final customers: metering and consumption data as well as data required for customer switching, demand response and other services	Regulation (EU) 2019/944
Operators of smart metering system	Data on the electricity they fed into the grid and their electricity consumption data shall be made available to final consumers, in accordance with the implementing acts adopted pursuant to Article 24 of the Directive, through a standardised communication interface or through remote access, or to a third party acting on their behalf, in an easily understandable format allowing them to compare offers on a like-for-like basis;	Directive (EU) 2019/944
TSO	Responsible for data management, including the development of data management systems, cybersecurity and data protection, subject to the applicable rules, and without prejudice to the competence of other authorities	Directive (EU) 2019/944
ENTSO-E	Promote cyber security and data protection in cooperation with relevant authorities and regulated entities;	Regulation (EU) 2019/943
Penalties		
Regulatory authority	Impose effective, proportionate and dissuasive penalties to regulated parties (electricity undertakings, transmission system owners, independent system operators etc.) for failing to comply with their obligations (or to propose that a competent court impose such penalties on them)	Directive (EU) 2019/944

4.4 Cross-Border data flows

The EU legislation recognizes that free flow of data within the internal EU market would help to remove obstacles to trade and distortions of competition and to prevent the emergence of further likely obstacles to trade and significant distortions of competition.

Regulation (EU) 2016/679 (GDPR) lays down rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data.

Regulation (EU) 2018/1807 sets up rules for non-personal data flow and the competencies of participating parties. Together with Regulation (EU) 2016/679 they provide a coherent set of rules that cater for free movement of different types of data.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)

- The protection of natural persons in relation to the processing of personal data is a fundamental right. This right is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.
- The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons about the processing of personal data.
- In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation
- The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union

- Aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users.
- Establishes the same principle of free movement within the Union for non-personal data as Regulation (EU) 2016/679, except when a restriction or a prohibition is justified by public security reasons.

Table 4.4: Cross Border flow of Personal Data

CROSSS-BORDER FLOW OF PERSONAL DATA	
Competent body	**Description**
National supervisory authorities	• Should monitor the application of the regulation and contribute to its consistent application in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market
Member states	• May conclude international agreements, which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect the Regulation (EU) 2016/679 and include an appropriate level of protection for the fundamental rights of the data subjects
Data controller or processor	• May transfer personal data to a third country or an international organisation only if they have provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available (given by Regulation).
Data controller processor	• Any specific authorization is not required for the transfer of personal data to a third country or an international organisation, where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Commission may review and amend or suspend such decision (without retro-active effect)

Table 4.5: Transnational Flow of non-personal Data

TRANS-NATIONAL FLOW OF NON-PERSONAL DATA	
Competent body	**Description**
Competent authorities	• Should have the power to request, or obtain, access to data for the performance of their official duties in accordance with Union or national law. Access to data by competent authorities may not be refused on the basis that the data are processed in another Member State.
Member states	• May impose effective, proportionate and dissuasive penalties for failure to comply with an obligation to provide data, in accordance with Union and national law.
European Commission	• Is encouraging development of self-regulatory codes of conduct covering, i.a. the aspect of creating approaches to certification schemes that facilitate the comparison of data processing products and services for professional users to facilitate the comparability of those products and services. Such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management

Directive 96/9/EC on the legal protection of databases

- Databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection
- The author of a database shall be the natural person or group of natural persons who created the base or, where the legislation of the Member States so permits, the legal person designated as the right holder by that legislation
- In respect of a database created by a group of natural persons jointly, the exclusive rights shall be owned jointly

5 FURTHER RECOMMENDED REFERENCES

Probably the most interesting reference to prepare terms for data sharing agreements is the **Support Center for data sharing**. It contains legal and technical data sharing reports, with detailed information about data sharing, it also provides models for data sharing, offering help by providing tools such as an API Licensing Assistant support [23].

- The IEA PVPS report on **data models for PV systems** also offers best practices and recommendations on data models and data acquisition [24]
- "The European **Data Flow Monitoring**": provides a tool for visualisation and monitoring of volume and patterns in data flows across EU [25]
- Horizon 2020 **Data Management Plans** presents compliance guidelines for following the GDPR [26]
- General **Data Protection Regulation** (GDPR) Compliance Guidelines [27]
- Guidance on **sharing private data** in the European data economy can be found in the following reference [28]
- **Business-to-Business data sharing**: an economic and legal analysis: (1) report by the JRC dating from 2020. It provides a lot of insights into the economics of data, examining the obstacles for B2B data sharing [29] (2) Report characterizing legal, technical and other types of barriers which currently prevent the full deployment of the European Data Economy and which limit Business to Business (B2B) data sharing and re-use in Europe [30]
- Till Jaeger, Legal Opinion – **Legal Aspects of European Energy Data** (2017). It addresses the legal situation of the reuse of data in both the European and Germany electricity markets. We focus on such data that is covered by transparency regulation [31]
- **An open data handbook:** featuring basic information about open data and more aspects, such as policy, standards, data training, right to information, privacy, civic engagement, an advocacy.
- **Open data for the energy sector (relevant for modelling of energy systems):** (1)report reviewing the legal status of publicly accessible data for modelling of energy systems. Relevant for databases [32]
- International **data spaces** [33]
- **Data Spaces** – Gaia-X proposes an architecture for data sharing in an ecosystem on cloud/edge infrastructures [34] [35]
- **Distribution of software**: (1) reference including considerations about what goes into a software distribution agreement and whether software distribution is considered in the data streams [36] (2) short article providing clear definitions linked to the distribution of open software [37]

Various **EU research projects** have been dealing with data sharing aspects. A short list of projects featuring interesting reports about topics like data spaces, management of data in the energy sector (including defining interoperability specifications) are listed below:

- **Catalyst project**: aims to convert data centres in energy flexibility ecosystems, sustaining investments in RES and EE [38]
- **Bridge initiative**: aims at fostering exchange of information, experience, knowledge, and best practices amongst its members. Several research projects financed by the EU are participating in this initiative which also has a task force for standardizing data management. [39]
- **Dominoes project**: features an interesting report about a smart distribution grid: a market driven approach for the next generation of advanced operation models and services [40]
- **Flexunity project** presents legal and technical requirements for balancing markets [41]
- **Merlon project:** introduces an integrated modular local energy management framework for the holistic operational optimization of local energy systems in the presence of high shares of volatile distributed RES. [42]

6 REFERENCES

[1] R. G. E. B. G. G. R. L. J. V. L. Sandys, «A strategy for a Modern Digitased Energy System - Energy data taskforce report,» BEIS- Ofgem - Innovate UK, UK, 2021.

[2] «https://www.sap.com/insights/what-is-data-governance.html,» SAP. [En ligne].

[3] Gaia-X, «Data Spaces,» Gaia-X European Association for Data and Cloud ASBL, [En ligne]. Available: https://www.gaia-x.eu/what-is-gaia-x/data-spaces. [Accès le 15 12 2021].

[4] European Comission, «Comission Staff Working Document on Common European Data Spaces,» EC, Brussels, 2022.

[5] Data Pitch Innovation Programme, «About data sharing,» data pitch , [En ligne]. Available: https://datapitch.eu/toolkit-about-data-sharing/. [Accès le 16 12 2021].

[6] EC, «Towards a European strategy on business-to-govenrment data sharing for the public interest,» European Union, Brussels, 2020.

[7] «Privacy Policies,» 2021. [En ligne]. Available: www.privacypolicies.com/blog/eula-vs-terms-conditions. [Accès le 28 01 2022].

[8] DG Connect - Support Center for Data Sharing, «B2- Analytical report on EU law applicable to sharing of non-personal data,» EC, Brussels, 2020.

[9] EC, «GDPR Regulation (EU) 2016/679,» 2016. [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[10] EC, «TFEU :Consolidated Version of the Treaty on the Functioning of the European Union,» EC, 2020. [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E/TXT.

[11] EC, «Database Directive: Directive 96/9/EC,» 1996. [En ligne]. Available: https://eur-lex.europa.eu/eli/dir/1996/9.

[12] L. Hirth, «Open data for electricity modeling: Legal aspects,» *Energy Strategy Reviews,* vol. 27, January 2020.

[13] EC, «Directive on Copyright in the Digital Single Market,» EC, 2019. [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0790.

[14] EC, «Regulation for the free flow of non-personal data in the EU,» EC, 2018. [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807.

[15] EC, «Directive 2009/24/EC,» 2009. [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009L0024.

[16] ISO, «ISO/IEC 38505-1:2017. Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data,» ISO, 2017.

[17] EC, «COMMISSION REGULATION (EU) No 543/2013,» 2013. [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02013R0543-20200101.

[18] [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_363_R_0009&from=EN.

[19] EC, «Proposal for a regulation on European Data Governance - Data Governance Act,» 2020. [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767.

[20] Go FAIR, «Fair principles,» Go FAIR, [En ligne]. Available: https://www.go-fair.org/fair-principles/. [Accès le 2021].

[21] BBC, «Copyright and intellectual property,» [En ligne]. Available: https://www.bbc.co.uk/bitesize/guides/zchcwmn/revision/3. [Accès le 15 12 2021].

[22] M. ,. D. M. ,. A. Wilkinson, «The FAIR Guiding Principles for scientific data management and stewardship,» *Sci Data 3,* vol. 3, 2016.

[23] SCDS, «Support Center for Data Sharing,» SCDS, [En ligne]. Available: https://eudatasharing.eu. [Accès le 12 01 2022].

[24] IEA PVPS T1/T14, «Data models for PV systems, Data models and Data Acquisition for PV registration schemes and grid connection evaluations - Best practice and recommendations,» IEA PVPS T1/T14-01:2020, 2020.

[25] EC, «European Data Flow Monitoring,» EC, [En ligne]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-data-flow-monitoring. [Accès le 12 01 2022].

[26] EC, «Data Management,» EC, [En ligne]. Available: • https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm. [Accès le 17 11 2021].

[27] EC, [En ligne]. Available: https://gdpr.eu.

[28] EC, «Private Data sharing in the European Data Economy,» EC, [En ligne]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2. [Accès le 17 11 2021].

[29] JRC, «Business-to-Business data sharing: an economic and legal analysis,» EU Science Hub, Seville, 2020.

[30] Deloitte /EC, «Study on emerging issues of data onwership, interoperability, (re-)usability, and access to data and liability,» EC DG communication networks, 2016.

[31] T. Jaeger, «Legal Opinion – Legal Aspects of European Energy Data,» EC, Copenhagen, 2017.

[32] L. Hirth, «Open data for electricity modeling: Legal aspects,» *Energy Strategy Reviews,* vol. 27, n° %1100433, 2020.

[33] «International data spaces,» [En ligne]. Available: https://internationaldataspaces.org/publications/papers-studies/. [Accès le 15 12 2021].

[34] Gaia-X, «Data Spaces,» [En ligne]. Available: https://www.gaia-x.eu/what-is-gaia-x/data-spaces. [Accès le 13 10 2021].

[35] Fiware - Open Compute project - Gaia X, «Smart digital economy - What has open source gotta do with it?,» Fiware, 2022.

[36] R. DeLoe, «Making the most of your software distribution agreement,» Legalzoom, 16 03 2021. [En ligne]. Available: https://www.legalzoom.com/articles/making-the-most-of-your-software-distribution-agreement. [Accès le 15 12 2021].

[37] L. Rosen, «Distribution of Software,» chez *Open Source Licensing*, Upper Saddle River, Prentice Hall PTR, 2004, pp. 41-50.

[38] Catalyst project, «Catalyst project presentation,» [En ligne]. Available: https://project-catalyst.eu/. [Accès le 17 11 2021].

[39] Bridge Initiative, «Data Management,» [En ligne]. Available: https://www.h2020-bridge.eu/working-groups/data-management/. [Accès le 17 11 2021].

[40] Dominoes project, «Deliverables; Smart distribution grids,» [En ligne]. Available: http://dominoesproject.eu/deliverables/. [Accès le 28 10 2021].

[41] Flexunity project, «Legal and technical requirements for balancing markets,» [En ligne]. Available: https://www.flexunity.eu/deliverables. [Accès le 28 10 2021].

[42] Merlon project, «Merlon - Deliverables,» [En ligne]. Available: https://www.merlon-project.eu/. [Accès le 13 10 2021].

[43] R. Kemp, «Legal aspects of managing data,» October 2019. [En ligne]. Available: www.kempitlaw.com. [Accès le 15 12 2021].

[44] EC, «Comission Staff working document: "Guidance on sharing private sector data in the EU data economy",» Brussels, 2018.