BD4NRG
Big Data for Next Generation Energy

Deliverable No. 2.4: BD4NRG Security, Privacy, Standards & Regulatory Compliance Specs

WP2 – System Requirements and Specifications

July 2021

www.bd4nrg.eu

Disclaimer

The BD4NRG project is co-funded by the Horizon 2020 Programme of the European Union. This document reflects only authors' views. The European Commission is not liable for any use that may be done of the information contained therein.

Copyright Message

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613

Grant Agreement Number: 872613 Acronym: BD4NRG

Full Title	Big Data for Next Generation Energy		
Topic	DT-ICT-11-2019 | Big data solutions for energy		
Funding scheme	H2020- IA: Innovation Action		
Start Date	January 2021	Duration	36
Project URL	www.bd4nrg.eu		
Project Coordinator	ENG		
Deliverable	D2.4- BD4NRG Security, Privacy, Standards & Regulatory Compliance Specs		
Work Package	WP2 - System Requirements and Specifications		
Delivery Month (DoA)	M7	Version	1.0
Actual Delivery Date	30/07/2021		
Nature	Report	Dissemination Level	Public
Lead Beneficiary	ELEX		
Authors	Giovanni Maria Riccio, Adriana Peduto, Jacopo Purificati, Carmela Occhipinti (ELEX), Alexander Pastor, Katharina Wehrmeister (RWTH), Marco Antonio Bucarelli (ASM), Miha Becan (ELES)		
Quality Reviewer(s):	Nikos Bilidis (ED), Elisa Herrmann (ATOS)		
Keywords	Security Requirements, Privacy Requirements, Standards, Requirements, legislative frameworks, NISD, GDPR, Third Energy Package, Electricity Network Codes and Guidelines, Methodology, BD4NRG Scenarios and Data, BD4NRG Compliance Best Practices		

Preface

BD4NRG focuses on addressing emerging challenges in big data management for energy sector with an innovative open holistic solution for smart grid-tailored, near real time, energy-specific and AI-based open Big Data Analytics modular framework. The vision is to deliver holistic services for techno-economic optimal management of Electric Power and Energy Systems (EPES) value chain. Services range from optimal risk assessment for energy efficiency investments planning, to optimized management of grid and non-grid owned assets, improved efficiency, and reliability of electricity networks operation, while at the same time contributing to achieve fair energy prices to the consumers and laying the foundations for an EU-level energy-tailored data sharing economy. The BD4NRG Toolbox will be implemented and validated in real-life pilots in 12 large-scale demo sites across 10 countries for:

- Increasing the efficiency and reliability of the electricity network BD-4-NET
- Optimising the management of assets connected to the grid BD-4-DER
- De-risking investments in energy efficiency and increasing the efficiency and comfort of buildings BD-4-ENEF

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

Who We Are

	Participant Name	Short Name	Country Code	Logo
1	ENGINEERING – INGEGNERIA INFORMATICA SPA	**ENG**	IT	
2	NATIONAL TECHNICAL UNIVERSITY OF ATHENS	**NTUA**	GR	
3	RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN	**RWTH**	DE	
4	EUROPEAN DYNAMICS LUXEMBOURG SA	**ED**	LU	
5	INTERNATIONAL DATA SPACES EV	**IDSA**	DE	
6	EUROPEAN NETWORK OF TRANSMISSION SYSTEM OPERATORS FOR ELECTRICITY AISBL	**ENTSO-E**	BE	
7	PANEPISTIMIO DYTIKIS ATTIKIS	**UNIWA**	GR	
8	ATOS SPAIN SA	**ATOS**	ES	
9	FUNDACION CARTIF	**CARTIF**	ES	
10	UNIVERZA V LJUBLJANI	**UNILJ**	SL	
11	ENEL X SRL	**ENELX**	IT	
12	REN - REDE ELECTRICA NACIONAL SA	**REN**	PT	
13	CENTRO DE INVESTIGACAO EM ENERGIA REN - STATE GRID SA	**RDN**	PT	
14	UNINOVA-INSTITUTO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIASASSOCIACAO	**UNINOVA**	PT	
15	ENERCOUTIM - ASSOCIACAO EMPRESARIALDE ENERGIA SOLAR DE ALCOUTIM	**ENERC**	PT	
16	FIWARE FOUNDATION EV	**FIWARE**	DE	
17	CENTRICA BUSINESS SOLUTIONS BELGIUM	**CENTRICA**	BE	
18	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	**TNO**	NL	
19	ASM TERNI SPA	**ASM**	IT	

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

	Participant Name	Short Name	Country Code	Logo
20	VIDES INVESTICIJU FONDS SIA	**LEIF**	LV	
21	COMSENSUS, KOMUNIKACIJE IN SENZORIKA, DOO	**COMSENSUS**	SL	
22	HOLISTIC IKE	**HOLISTIC**	GR	
23	INTERUNIVERSITAIR MICRO-ELECTRONICA CENTRUM	**IMEC**	BE	
24	TERRASIGNA SRL	**TS**	RO	
25	UBIMET GMBH	**UBIMET**	AT	
26	ELEKTRO LJUBLJANA PODJETJE ZADISTRIBUCIJO ELEKTRICNE ENERGIJE D.D.	**EKL**	SL	
27	BORZEN, OPERATER TRGA Z ELEKTRIKO, D.O.O.	**BORZEN**	SL	
28	AJUNTAMIENTO DE SANT CUGAT DEL VALLES	**AJSCV**	ES	
29	ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA	**ELES**	SL	
30	E-LEX - STUDIO LEGALE	**ELEX**	IT	
31	OSMANGAZI ELEKTRIK DAGITIM ANONIM SIRKETI	**OEDAS**	TR	
32	VEOLIA SERVICIOS LECAM SOCIEDAD ANONIMA UNIPERSONAL	**VEOLIA**	ES	
33	STICHTING EG	**EGI**	NL	
34	CINTECH SOLUTIONS LTD	**CN**	CY	
35	EMOTION SRL	**EMOT**	IT	

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

Contents

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

Figures

Tables

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

Executive summary

This deliverable is the result of the specification activities performed in Task 2.5 “BD4NRG Security, Privacy, Standards & Regulatory Compliance Specs”. This deliverable will specify the requirements related to the security, privacy, to be taken into account in the BD4NRG system implementation. It follows the definition of the ethics requirements in WP11, and the data management plan in WP6.

Based on these relevant inputs, and on additional analysis of the use case scenarios, data types, and involved actors, this deliverable provides reader with:

i. an analysis of well-proven technologies and standards to be applied to data (e.g. anonymization, aggregation, minimization), taking into account possible ethical issues as well;

ii. an analysis of data protection needs and the available standards, policies and methodologies about the data acquisition, data management and data access, in order to guarantee the user’s data ownership and governance;

iii. an analysis of current EU and international legislative frameworks that concern network and information security (e.g. NISD - Network and Information Security Directive), but also taking into consideration legislative requirements that affect the Electrical Power and Energy System (EPES) sector (e.g. GDPR - General Data Protection Regulation, Third Energy Package, and the Electricity Network Codes and Guidelines).

iv. security and privacy of data guidelines and rationale behind them. This latest part will constitute an extractable handbook for the whole technical development team to be used as a reference guide.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

Acronyms and abbreviations

Table 1 - Acronyms and Abbreviations used in D2.4

Acronym	Description
AMR	Automatic Meter Reading
BESS	Battery Energy Storage System
BMS	Battery Management System
BZs	Bidding zones
CBs	Circuit Breakers
CCRs	Capacity Calculation Regions
CSIRT	Computer Security Incident Response Team
DER	Distributed Energy Resource
DR	Demand Response
DSO	Distribution System Operator
ENISA	European Network and Information Security Agency
EPES	Electrical Power and Energy System
ERP	Enterprise Resource Planning
EV	Electric Vehicle
GDPR	General Data Protection Regulation - Regulation (EU) 2016/679
GIS	Geographic Information System
GLs	Guidelines
HV	High Voltage
LFC	Load Frequency Control
LSP	Large Scale Pilot
LV	Low Voltage
MDMS	Meter Data Management System
MV	Medium Voltage

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

NCs	Network Codes
NISD	Network and Information Security Directive – Directive (EU) 2016/1148
RES	Renewable Energy Source
TCMs	Terms and Conditions or Methodologies
TSO	Transmission System Operator
UC	Use Case
VPP	Virtual Power Plant

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

1 Introduction

The identification and specification of privacy and security requirements are the main topics of this document. These special requirements have to be taken into account in the BD4NRG system implementation, together with the functional and non-functional requirements coming from the development activities.

Requirements are identified and specified based on specific BD4NRG use case scenarios and how their actors will deal with specific data types and data flow, so to guarantee compliance with current EU and international legislative frameworks (e.g. NISD, GDPR, Third Energy Package, and the Electricity Network Codes and Guidelines).

The document is organised in chapter listing and/or describing the following topics:

Table 2 – D2.4 chapters and description

Chapter	Topics description
1 – Introduction	Structure of the deliverable
2 – Methodology	Methodology adopted for the identification and specification of privacy and security requirements process
3 – BD4NRG Legal Framework	Definition of the BD4NRG data protection legal framework, in order to guarantee compliance with the current privacy and data protection legal framework, including GDPR. Moreover an analysis of the electricity codes and guidelines is performed.
4 – BD4NRG Security Framework	Definition of the BD4NRG security framework, reporting the current security framework, in the context of electricity, including NISD.
5 - BD4NRG Scenarios and Data types	Analysis of the BD4NRG use case scenarios, involved actors, and their related data types, in order to identify potential legal and/or security concerns.
6 - BD4NRG Compliance best practice	Definition of BD4NRG Compliance best practice to be adopted by the BD4NRG technical development team for the system design and implementation
7 – Conclusions	Conclusions of the deliverable
8 – References	List of references used for this deliverable

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

2 Methodology

The methodology adopted in BD4NRG project for the identification and specification of legal and security concerns is based on a three-steps process, where the conceptual framework constitutes the foundation (see Figure 1).

Figure 1 – BD4NRG Legal and Security Specification Methodology

The conceptual framework provides an outlook on the legal regulations and security standards to be applied for the specific BD4NRG objectives, use case scenarios and technology implementation. This conceptual framework provides the BD4NRG consortium with **compliance rules and governance policies** to be followed during the whole project lifecycle. For defining the conceptual framework, BD4NRG is using references such as GDPR, Third Electricity Package, Electricity Network Codes and Guidelines, and NISD.

This conceptual framework is consequently instantiated by analysing **BD4NRG scenarios and data types**. This analysis doesn't aim to replicate the technical details of use case scenarios from the requirements specifications or the data types from the data management plan, on the other hand it uses these technical documents as inputs for a preliminary assessment of technical specification and the identification of **potential concerns** (i.e. privacy, security) with respect to the established conceptual framework, as well as suggesting countermeasures.

For performing the analysis of BD4NRG scenarios and data types, a use case datasheet template has been defined, as shown in Table 3. This template is a simple and effective tool for monitoring and assessing potential concerns, and if necessary, partners will update during the project lifecycle with further details.

Table 3 – Scenarios and Data Types Sheet template

LSP – UC	**<LSP number – UseCase number and title>**
UC Description	<Short description of the UC in less than 3 rows>
UC Owner	<UC Owner>
Data Subject Type	Options: {EnergyGeneration, EnergyTransmission, EnergyDistribution, ResidentialCustomer, IndustrialCustomer}
Data Subject Description	The entity from whom or about whom the project collects information in connection with its activities. <Short description of the data subject, e.g. TSO in country X, DSO in country Y, …>
Data Source(s)	<List here the data source(s) e.g. Smart Meter in primary station, Circuit Breaker in secondary station, …>

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

Data Controller	The entity that determines the why (purpose) and the how (terms and conditions) for processing data <Short description of the data subject, e.g. TSO in country X, DSO in country Y, …>
Personal Data	Yes / No / NA
Personal Data Protection Mechanisms	If data contain personal data, specifies the purpose and the designed mechanisms to be applied Options: {Anonymisation, Peudonymisation, Aggregation, Minimisation}
Potential Concerns	Based on analysis of the above information, identified potential concerns w.r.t. conceptual framework, in terms of likelihood and impact.

Finally, the specification closes with the definition of a summary of **compliance best practices**. Some of them have been already anticipated at the beginning of the project with a short presentation, and for this reason, this document provides the reader with the rationale behind these best practices and provides further and useful insights.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

3 BD4NRG legal framework

3.1 BD4NRG data protection legal framework

In the context of BD4NRG, a tailored data protection legal framework is depicted according to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as: GDPR) [2]. Without providing details on this relevant EU regulation, the following subsections provides the reader with energy-domain specific details, relevant to the project activities, its use case scenarios and expected outcomes.

3.1.1 Personal data and personally identifiable data

GDPR is the last step of a complex framework that the European institutions have drafted for the regulation of personal data, privacy and security.

The GDPR, as it will be explained afterwards is a legislative text which is directly applicable, without any need of formal transposition into the member States' legislation, within all the EU territory.

GDPR defines (article 4, par. 1) the personal data 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*".

Article 4 of the GDPR includes definitions of specific personal data, which are mostly related to sensitive and specific aspects of the personality of physical subjects, and notably:

- genetic data: *personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question* [article 4, n. (13)];

- biometric data: *personal data resulting from specific technical processing relating to the physical, physio- logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data* [article 4, n. (14)];

- data concerning health: *personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status* [article 4, n. (15)].

Furthermore, processing of personal data being able to reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are, in general, prohibited and may be processed exclusively in some specific cases. These categories of personal data that are subject to additional protections, as they are considered as the hardcore of the protection that must be ensured to citizens by privacy regulations.

The general principle is that personal data can be processed if the data subjects have provided their consent to the processing of their personal data for one or more specific purposes. However, the GDPR lists several cases in which personal data may be processed based on other circumstances and prerequisites, such as where processing is necessary to protect the vital interests of the data subject or of another natural person where the

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

data subject is physically or legally incapable of giving consent.

Anonymous information is not covered by the EU Regulation. Whereas n. 26 states that "*The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes*".

The GDPR makes a distinction between the anonymization and the pseudoanonymization. The latter refers to the reversible de-identification of personal data, for example in case where it is allowed to re-identify hashed identifiers.

Furthermore, according to n. 26 of the GDPR,

"*The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes*".

It is a crucial point for the use of big data as personal data, once anonymized (or pseudo-anonymized), may be freely processed, without any prior authorization by the data subject.

Even if the GDPR does not define the anonymized data, it includes a definition of pseudononimization which 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

3.1.1.1 Personal data in smart grids

In 2009 the European Commission set up the Smart Grid Task Force to advise on issues related to smart grid deployment and development and help shape EU smart grid policies.

It currently consists of five Expert Groups which focus on specific areas, including Expert Group 2 – Regulatory recommendations for privacy, data protection and cyber-security in the smart grid environment. This group provided a non-exhaustive example of personal data [3] as follows:

- Household and organisations consumption;
- Consumer registration data: names and addresses of data subjects, etc.;
- Usage data (energy consumption, demand information and time stamps), as these provide insight in the daily life of the data subject;

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

- Amount of energy and power (e.g. kW) provided to the grid (energy production), as they provide insight into the amount of available sustainable energy resources of the data subject;
- Locally produced weather forecast – consumption prediction / forecasts;
- Demand forecast of building, campus and organisation;
- Technical data (tamper alerts), as these might change how the data subject is approached;
- Profile of types of consumers, as they might influence how the consumer is approached;
- Data and function of individual consumers / loads;
- Facility operations profile data (e.g. hours of use, how many occupants at what time and type of occupants);
- Frequency of transmission of data (if bound to certain thresholds), as these might provide insight in the daily life of the data subject;
- Billing data and consumer's payment method.

3.1.2 Data roles

Before considering the specific issues concerning the processing of personal data in the smart grids context, it is necessary to list the definitions of data subject, data controller, data processor, third party and recipient within the GDPR.

Within the data protection regulation, the data subject is a living individual and a natural person to whom personal data are referred.

The data controller (or simply the "controller") is the subject (natural person or legal entity), public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In other words, the data controller is the one who is directly responsible for the processing, for its purposes, for the security measures, and so on.

The data controller may appoint some tasks in the processing to another subject who is qualified by the GDPR as the data processor (or simply the "processor") who is the one who processes personal data on behalf of the controller. The processor may be an internal subject belonging to the entity which acts as controller or an external subject (e.g. the company who is in charge for security measures; suppliers of external services, etc.).

Personal data may be disclosed to other subjects. In this case, their role, in the context of GDPR, is defined as recipient, i.e. a "*natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing*".

Finally, the third party is defined by the GDPR as "*a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data*".

3.1.2.1 Data roles in smart grids

The Expert Group 1 – Standards and Interoperability for Smart Grids Deployment, in the context of the Smart Grid Task Force set up by the European Commission in 2009, issued a report [4] in November 2016 where main roles in Smart Grids are explained.

The sources the report took into account are the GDPR, the Energy Efficiency Directive 2012/27/EU, the Electricity Directive 2009/72/EC and the Gas Directive 2009/73/EC. It also bases roles definition on other established role models in the European energy market, such as the harmonised electricity market role model from ENTSO-E, evolvDSO, or the DAMA/DMBOK.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

All these roles are mapped onto the GDPR, reporting an example list of roles:

- The data subject could be considered as the customer or the party connected to the grid.
- The controller could be considered as the party responsible for data management (partly) or the metered data responsible.
- The processor could be considered as the party responsible for data management (partly), metered data collector or metered data aggregator.

3.1.3 Consent

As said, the general rule holds that consent is required in order to process personal data. Consent is not necessarily in written, but must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous willing.

In some specific cases – e.g. where personal data are required for the execution of a contract agreed with the data subject – consent is not required.

3.1.3.1 Consent in smart grids

According to [4], the mechanisms related to the consent in Smart Grids are explained as follow:

- The **Data Subject** (i.e. the energy services Customer) gives or withdraws consent to and requests information/actions from the Data Controller (or a set of coordinated Controllers).
- The **Data Controller** provides the Customer with relevant information, determines the purposes and means of the processing of his/her data (saved in the Customer Data Repository) and manages the Consent Register.
- The Consent Register can be consulted/accessed by authorized **Processors** such as for instance the Metered data collector, the Metered data responsible and the Metered data aggregator, as well as by **Third Parties** such as the Energy Service Operators.
- The Customer Data Repository stores personal data of the Data Subject and provides him/her access to all the saved data.
- The Customer Data Repository can be accessed/consulted by
    - authorised Processors that process data on behalf of the Controller
    - Third Parties in coordination with the Controller for the exchange of customer data
    - **Recipients** to which customer data is provided.
- Both the Controller and the Processor inform, advise and coordinate their activity with the Data Protection Officer, that communicates with the Supervisory Authority.

Data Management

The reform introduced by the GDPR is designed to provide EU citizens with more control over their own personal data.

The scope of personal data has been expanded, including anything that can uniquely identify an individual, 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 individual.

Moreover, as for art. 5, Personal data shall be:

- *processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');*
- *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation'**);*

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

- *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation**’)*;
- *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘**accuracy**’)*;
- *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘**storage limitation**’)*;
- *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality**’)*.
- *the controller shall be responsible for, and be able to demonstrate compliance with ‘**accountability**’*.

Moreover, the GDPR introduces a range of requirements, constraints and controls to govern how personal data should be collected, stored, processed, retained, and shared as hereafter listed:

- Individuals must provide explicit consent to data collection – “consent by default” is no longer valid. The organization seeking consent must also provide clear information on how that data will be used, for how long it will be retained, and how it will be shared with third parties. Individuals can retract consent at any time, without prejudice. Additional permissions must be requested from the individual if the data is to be used for processing purposes beyond the original consent.
- Data protection has to be by design and by default, requiring data protection mechanisms to be embedded into products and services from the earliest stage of development, and the adoption of strictest privacy settings without any manual input from the end user.
- Individuals have the "right to be forgotten", also known as “right to erasure”, so that there is no legitimate reason for an organization to refuse the request of individuals to definitely remove their personal data when they ask for it to no longer be retained.
- Individuals should have easier access to their data, enabling them to review what data is stored about them and how it is processed, who it is shared with, along with the ability to migrate that data between service providers without restriction.
- Organisations should conduct a Data Protection Impact Assessment to understand personal data risk exposure.

Finally, in case of data breach, **disclosure within 72 hours** must be made to the competent Data Protection Authority, enabling individuals to be informed and take appropriate remedial action, while in case of organisations’ non-compliance with the GDPR provisions, substantial financial recourse will be made against them.

3.2 BD4NRG electricity codes and guidelines

The European Union’s legal framework for electricity originated in the Third Energy Package legislation of 2009. This framework has recently been adjusted by the legislation forming the Clean Energy Package (CEP), and such amendments came into force in January 2020. Like every EU Regulation, the Package Regulations are legally binding, directly applicable, and enforceable by Member States.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

Since the aim of the mentioned Packages is to harmonize rules and principles on the subject for all EU Member States, most of the provisions laid down in the legislation are addressed to the legislative bodies of the Member States, which may specify the contents by internal provisions.

Nonetheless, the Packages contain provisions requiring the adoption of further technical, delegated legislation in the form of either Network Codes (NCs) or Guidelines (GLs). The Regulations also establish the methodology for the drafting and the adoption of NCs or GLs, which is based on the the EU "Comitology" procedure and includes a wide range of views and stakeholders (transmission system operators, nominated electricity market operators, national regulatory authorities, ACER - Agency for the Cooperation of Energy Regulators, and the European Commission). Based on the Third Energy Package, four GLs and four NCs were adopted. This first generation of measures are categorized into network connection rules, system operation rules and market rules. The current framework for these instruments is therefore composed as follows.

3.2.1 Network codes

- Commission Regulation (EU) 2016/631 establishing a network code on requirements for grid connection of generators;
- Commission Regulation (EU) 2016/1388 establishing a network code on demand connection;
- Commission Regulation (EU) 2016/1447 establishing a network code on requirements for grid connection of high voltage direct current systems and direct current-connected power park modules;
- Commission Regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration.

3.2.2 Guidelines

- Commission Regulation (EU) 2015/1222 establishing a guideline on capacity allocation and congestion management;
- Commission Regulation (EU) 2016/1719 establishing a guideline on forward capacity allocation;
- Commission Regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation;
- Commission Regulation (EU) 2017/2195 establishing a guideline on electricity balancing.

Network Codes (NCs) and Guidelines (GLs) are binding EU Regulations of the European Commission, containing common technical and commercial rules, with the primary objective of fostering the integration of national electricity markets across Europe, thus creating a well-functioning internal energy market.

These instruments are without prejudice to the right of Member States to establish national network codes, provided that these do not relate to cross-border trade. In case of conflict, in fact, EU Regulations prevail over domestic legislation, which would then cease to apply. NCs and GLs divide the EU territory into 10 capacity calculation regions (CCRs), 32 bidding zones (BZs), as well as many balancing areas, synchronous areas, and load frequency control blocks (LFC blocks). From this subdivision emerges a picture that is certainly fragmented and variable in space and time. It is therefore necessary to consider and address the technical differences between these areas and regions. In this regard, while the NCs contain more directly applicable rules, the GLs merely outline a framework within which a separate category of regulatory tools is developed: the Terms and Conditions or Methodologies (TCMs). The hierarchical framework of the relevant provisions should therefore be reconstructed as follows. The Energy Package contains the general principles for the electricity sector; NCs and GLs are complementary to these general principles and do not contradict them; lastly, the TCMs are tools to implement the aforementioned instruments and cannot overrule either the NCs and GLs or the provisions of the Energy Package.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

4 BD4NRG security framework

4.1 BD4NRG security and NISD

The Directive 2016/1148 on security of network and information systems ("NIS Directive" or "NISD")[3] has been adopted as part of the European strategy aimed at strengthening cyber-security and IT resilience of the European Union and moves from the view that networks, systems and information services play a vital role in a modern society and therefore it is essential that they are reliable and safe for economic and social activities, in particular for the purposes of the functioning of the market.

In particular, the purpose of the NIS Directive is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at a cross-border level.

4.1.1 The scope of NIS Directive

NIS Directive (NISD) applies to operators of essential services and digital service providers.

With reference to the operators of essential services (i.e. energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure), Article 5(2), NISD provides the criteria for their identification as follows:

i. provides a service which is essential for the maintenance of critical societal and/or economic activities;
ii. the provision of that service depends on network and information systems; and
iii. an incident would have significant disruptive effects on the provision of that service.

It is important to remark that, starting from November 2018, Member States had to identify the operators of essential services with an establishment on their territory, supported by procedures defined in Directive 2015/1535[6] as well.

The identification of Operators of Essential Services (OESs) is still a critical aspect. The Figure 2 (Source:[7]) remarks how numbers of OES identified by Member States across all sectors (per 100.000 inhabitants) differ across the EU contries.

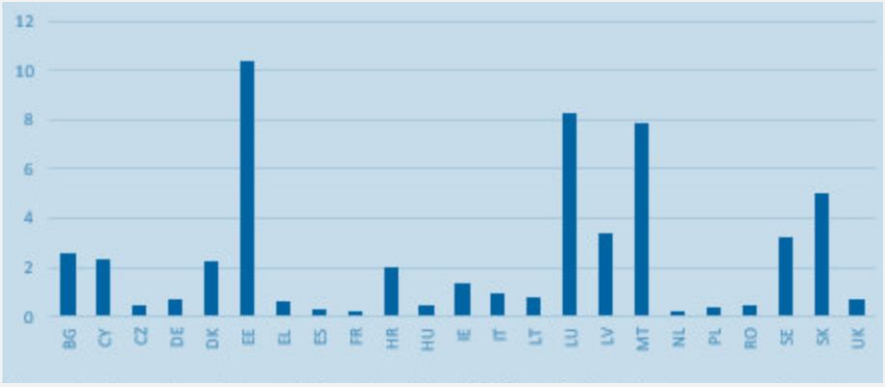

Figure 2 – OESs identified by Member States across all sectors, per 100.000 inhabitants.

In particular, pursuant to Article 4(1) no 6, NISD a "digital service provider" is a legal person who offers a digital service, whereby "service" means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (mainly online marketplace, online search engine, cloud computing).

As above-mentioned, the NIS Directive is intended to establish a high common level of network and information security throughout the EU, aiming at increasing the overall level of IT security by ensuring:

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

a. that Member States provide appropriate tools, for example by designating a Computer Security Incident Response Team ("CSIRT") and a national competent authority for network and information security;
b. that Member States cooperate with each other by setting up a cooperation group – the Commission and the European Network and Information Security Agency ("ENISA") composed by representatives of Member States - to support and facilitate strategic cooperation between countries in relation to the security of networks and information systems and to facilitate the exchange of information between Member States in order to increase confidence;
c. to develop a culture of security in areas that are vital for the economy and society, and that are based heavily on information and communication technologies such as transport, energy, banks, infrastructure financial markets, health and digital infrastructures.

Without prejudice to the minimum level of harmonisation laid down by the NISD, Member States are free to adopt standards which guarantee a higher level of protection.

4.1.2 Security requirements

According to the NISD, Member States have to ensure that operators of essential services and digital service providers adopt appropriate and proportionate technical and organizational measures to address the risks posed to network security and the information systems they use in their operations.

Given the most up-to-date knowledge on the subject, these measures ensure a level of network security and information systems appropriate to existing risk; to do that Member States must take into account the following elements:

a) the safety of systems and installations;
b) handling of accidents;
c) management of operational continuity;
d) monitoring, auditing and testing;
e) compliance with international standards.

The NIS Directive does not exhaust the IT security requirements, even those who are not obliged to comply with the NIS Directive's obligations may indeed be addressed by other standards that impose parallel obligations (e.g. minimum security requirements required to processing personal data).

4.1.3 Incident notification

Article 4(1) no 7, NISD defines "incident" as "any event having an actual adverse effect on the security of network and information systems".

On this point, in order to determine the significance of the impact of an incident, operators of essential services and digital service providers must take into account the following parameters:

i. the number of users affected by the disruption of the essential service;
ii. the duration of the incident; and
iii. the geographical spread with regard to the area affected by the incident.

The notification will have to take place without unjustified delay.

There is also a voluntary notification procedure that may be carried out by those who have not been identified as operators of essential services and are not digital service providers.

Without prejudice to the possibility for national States to adopt rules ensuring a higher level of protection than the NIS Directive, they may, on a voluntary basis, report incidents that have a significant impact on the continuity of the services they render.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

4.1.4 Data protection prospective

In many cases cyber attacks and incidents compromise personal data, therefore the NIS Directive states that competent authorities should work in close cooperation with the data protection authorities.
In this respect, both authorities should collaborate and exchange information on all relevant aspects to address personal data breaches caused by incidents.

It is important to point out that, currently, security incidents involving personal data are also regulated by the General Data Protection Regulation ("GDPR"), establishing a discipline on breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (the so-called "data breach" pursuant to Article 33, GDPR).

The two disciplines should not be confused as the GDPR and the NIS Directive have different objects and different scope.

Nevertheless, the two legislations may overlap when a security incident also implies a violation of personal data: in this case, public or private entities that provide the service affected by the accident (and the simultaneous breach of personal data) will have to fulfill the notification obligations provided by both NISD and GDPR.

4.1.5 Proposal for NIS 2 Directive

NISD is the first piece of EU-wide legislation on cybersecurity, specifically aiming at establishing a high common level of cybersecurity across the Member States. While NISD increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market [7]. To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, on 16th December 2020, the EU Commission adopted a proposal for a revised Directive on Security of Network and Information Systems (the so-called "NIS2 Directive") [8].

The new Commission proposal aims to address the deficiencies of the previous NIS Directive, inter-alia by:

i. expanding the scope and, in particular, adding new sectors and introducing a clear size cap;
ii. eliminating the distinction between operators of essential services and digital service providers;
iii. strengthening security requirements for the companies, in particular by imposing a risk management approach providing a minimum list of basic security elements that have to be applied;
iv. requiring individual companies to address cybersecurity risks in supply chains and supplier relationships;
v. introducing a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creating an EU registry on that operated by the ENISA.

The NIS2 Directive proposal shall be now subject to negotiations between the co-legislators (i.e. the Council of the EU and the European Parliament) and, once agreed and consequently adopted, Member States will have to transpose the NIS2 Directive within 18 months.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

5 BD4NRG scenarios and data types

The BD4NRG solutions will be applied, implemented, demonstrated and validated in real-life pilots in 12 large-scale pilots (LSPs) across 10 countries. The rationale of pilot applications is to address in a combined way two of the major challenges actually hindering big data analytics value capturing in smart energy grids, i.e.

i. nurturing the shifting towards predictive/prescriptive analytics, and
ii. enabling multiple data source analytics for multiple applications.

This section aims to analyse high priority and/or mature use case scenarios (available at the time of writing of this document) for identifying potential concerns with respect to the conceptual framework described in the above sections. Use case scenarios are described according to the template defined in section 2.

It is important to mark that in BD4NRG project, the consortium has confirmed that personal data will not be treated during the project lifecycle. This means that, even if some use cases could potentially consider manage personal data, this specific type of data will not be shared within the consortium, by adopting data protection mechanisms as well.

5.1 BD4NRG use case scenarios

LSP – UC	**LSP 1 – UC 1: AI methods applied to Condition-based monitoring of Circuit Breakers**			
UC Description	This UC analyzes Circuit Breakers (CBs) operating at High Voltage (HV) levels, applying data processing and data analytics tools to CB incident report data (faults).			
UC Owner	REN - TSO in Portugal RDN - technical partner in Portugal			
Data Subject Type	Energy Transmission			
Data Subject Description	REN - TSO in Portugal			
Data Source(s)	CB data: catalogue and technology type, criticality index, planned outages, daily operation registers, events from SCADA CB activation incident historic data: maintenance and fault records, failure notes, disturbance records in the form of oscillography data from current and voltage channels, number of operations and other sensor data			
Data Controller	REN - TSO in Portugal			
Personal Data	No			
Personal Data Protection Mechanisms	N/A			
Potential Concerns	**Likelihood**	Low	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 1 – UC 2: Semi-Automatic Maintenance Plan for Right-of-Ways (RoW) in Overhead Lines (OHL)			
UC Description	Analysis and supervision of OHLs operating at HV levels; identification of potential abnormalities such as stork nests, fiber optic boxes etc.			
UC Owner	REN - TSO in Portugal RDN - technical partner in Portugal			
Data Subject Type	Energy Transmission			
Data Subject Description	REN - TSO in Portugal External data			
Data Source(s)	LIDAR cylindrical scan data (point clouds) from transmission line towers Computer vision data Vegetation index (external) Climate data (external) Satellite data (external)			
Data Controller	REN - TSO in Portugal			
Personal Data	No			
Personal Data Protection Mechanisms	N/A			
Potential Concerns	**Likelihood**	Low	**Impact**	Low

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 2 – UC 1: Maintenance Plan Optimization			
UC Description	Several activities to optimize asset maintenance: (1) operation activities, (2) maintenance activities, (3) planning activities			
UC Owner	ELES - TSO in Slovenia			
Data Subject Type	Energy Transmission			
Data Subject Description	ELES - TSO in Slovenia			
Data Source(s)	Operational data from SCADA Diagnostics from monitoring systems measuring different parameters Periodic inspection data (visual, thermo-visual, chemical tests, electrical testing) Technical specifications of assets (CBs, isolating switches, instrument transformers, lightning arresters, power transformers) Data from maintenance (planned and on-demand; type of activity and cost)			
Data Controller	ELES - TSO in Slovenia			
Personal Data	No			
Personal Data Protection Mechanisms	In case of potential use of personal data (not expected), anonymization techniques will be applied			
Potential Concerns	**Likelihood**	Low	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 3 – UC 1: Efficient Management of Flexibility Resources for Supporting Grid Operation			
UC Description	Establish coordination between Electric Vehicles (EVs) and Renewable Energy Source (RES) to prevent overloading assets of the Low Voltage (LV) network (i.e., cables and transformers). To achieve this load and EV charging station forecasts are required.			
UC Owner	ASM - DSO in Italy			
Data Subject Type	Energy Distribution, Residential Customer, Business Customer			
Data Subject Description	ASM - DSO in Italy Business & residential customers (Terni, Italy)			
Data Source(s)	IoT smart meters (business and residential customers, x150) Concentrator-level PMUs (x2) District-level PMUs Primary substations (x3) Secondary substations (x600) Secondary substations with RTUs and other digital sensors (x2) Secondary substations with audio sensors (x10) collecting unstructured audio data (for prediction of abnormal noise patterns) Intelligent EV recharging stations (x5) EVs (x10)			
Data Controller	ASM - DSO in Italy			
Personal Data	Yes			
Personal Data Protection Mechanisms	Aggregation (average temperature in substation, average consumption/production, average charging session time, average charging cost, average session energy, aberage charging session CO_2 emissions)			
Potential Concerns	**Likelihood**	Medium	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 3 – UC 2: Anticipated Prediction of Asset Failures			
UC Description	A big data analysis should find correlations between measured LV quantities and faults in the power distribution network.			
UC Owner	ASM - DSO in Italy			
Data Subject Type	Energy Distribution, Residential Customer, Business Customer			
Data Subject Description	ASM - DSO in Italy Business & residential customers (Terni, Italy) UBIMET - Austrian meteorology company TS - Romanian earth observation company			
Data Source(s)	IoT smart meters (business and residential customers, x150) Concentrator-level PMUs (x2) District-level PMUs Primary substations (x3) Secondary substations (x600) Secondary substations with RTUs and other digital sensors (x2) Secondary substations with audio sensors (x10) collecting unstructured audio data (for prediction of abnormal noise patterns) Intelligent EV recharging stations (x5) EVs (x10) Weather data from UBIMET Geographical imagery from TS			
Data Controller	ASM - DSO in Italy			
Personal Data	Yes			
Personal Data Protection Mechanisms	Aggregation (average temperature in substation, average consumption/production, average charging session time, average charging cost, average session energy, average charging session CO_2 emissions)			
Potential Concerns	**Likelihood**	Medium	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 4 – UC 1: Predictive Maintenance and Fault Prediction for MV Grid and Cross-Functional Predictive Asset Management			
UC Description	This UC aims at reducing faults in Medium Voltage (MV) grids big data AI tools analyze long-term historical data to make short-term predictions which is then evaluated. The resulting AI will be used to predict future operation, maintenance and failure of MV network assets.			
UC Owner	OEDAS			
Data Subject Type	Energy Distribution			
Data Subject Description	OEDAS - DSO in Turkey External data			
Data Source(s)	SCADA & power quality analyzer data Automatic Meter Reading (AMR) Enterprise Resource Planning (ERP) Geographic Information System (GIS)			
Data Controller	OEDAS - DSO in Turkey			
Personal Data	Yes			
Personal Data Protection Mechanisms	Anonymization, Aggregation (to be defined for each specific dataset)			
Potential Concerns	**Likelihood**	High	**Impact**	Low

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 5 – UC 1: The agents responsible for controlling residential demand response assets can benefit from the transferred knowledge from other agents in an MDP setting.			
UC Description	This UC is about data-driven model building for LV/MV grid-flexibility. At this stage of the project, the exact asset portfolio (e.g., EV, electric boilers, etc.) has to be defined.			
UC Owner	CENTRICA - aggregator in Belgium			
Data Subject Type	Energy Distribution, Residential Customer			
Data Subject Description	Dutch and Belgian DSOs Residential DR asset owners			
Data Source(s)	Metering data, DR data, open data from Dutch and Belgian DSOs Time series data of flexible assets including voltage and power Smart meter data Residential DR assets (300++) Weather data Wholesale market data			
Data Controller	CENTRICA - aggregator in Belgium			
Personal Data	Yes			
Personal Data Protection Mechanisms	Anonymization, Aggregation depending on the dataset. However, personal data will not be shared and processed.			
Potential Concerns	**Likelihood**	Medium	**Impact**	High

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 5 – UC 2: Using residential DR assets to retrieve local grid information and use this information in the aggregation activations			
UC Description	Leveraging data collected by the flexibility provder to perform Demand Response (DR) in a grid-friendly way, i.e. such that is supports the grid, mitigating voltage and congestion issues.			
UC Owner	CENTRICA - aggregator in Belgium			
Data Subject Type	Energy Distribution, Energy Transmission, Residential Customer			
Data Subject Description	DSO(s) - unspecified TSO(s) - unspecified Residential			
Data Source(s)	DSO topology and measurement data Data or simulation model or congestion/voltage assumptions (Historical) time series data of flexible assets including voltage and power Smart meter data Residential DR assets (300++)			
Data Controller	CENTRICA - aggregator in Belgium			
Personal Data	Yes			
Personal Data Protection Mechanisms	Anonymization, Aggregation depending on the dataset. However, personal data will not be shared and processed.			
Potential Concerns	**Likelihood**	Medium	**Impact**	High

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 6 – UC 1: Identification of Flexibility Potential Based on Near Real-Time Data			
UC Description	This is UC is concerning integrating third-party owned small-scale RES and DR flexible assets into the DSO grid and facilitate a data-driven energy market that can operate closer to the margin.			
UC Owner	EKL - DSO in Slovenia BORZEN - Power Market Operator in Slovenia			
Data Subject Type	Energy Generation, Energy Distribution, Residential Customers			
Data Subject Description	EKL - DSO in Slovenia EV charging station owner(s) Smart meter owners			
Data Source(s)	Smart meter data from Meter Data Management System (MDMS) EV charging stations Field trial area power network model (topology, line paramters, instantaneous configuration) Raw data from power quality analyzers			
Data Controller	EKL - DSO in Slovenia			
Personal Data	No			
Personal Data Protection Mechanisms	Even if data sources can gather personal data, personal data will not be shared and processed.			
Potential Concerns	**Likelihood**	High	**Impact**	Low

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 6 – UC 2: Independent Aggregator Flexibility Activation, Quantification and Settlement			
UC Description	Main concerns of this UC are the quantification of service in energy terms, settlement models, impact on data flows and usage and appropriate simulation models when flexibility requests are triggered.			
UC Owner	EKL - DSO in Slovenia BORZEN - Power Market Operator in Slovenia			
Data Subject Type	Energy Generation, Energy Distribution, Residential Customers			
Data Subject Description	EKL - DSO in Slovenia EV charging station owner(s) Smart meter owners			
Data Source(s)	Historical datasets or simulation data (smart meters data from MDMS, EV charging stations, raw data from power quality analyzers, market data) Simulation models (if historical dataset not available)			
Data Controller	EKL - DSO in Slovenia			
Personal Data	No			
Personal Data Protection Mechanisms	Even if data sources can gather personal data, personal data will not be shared and processed.			
Potential Concerns	**Likelihood**	Medium	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 7 – UC 1: Predictive Analytics Forecasting of Storage-Optimized Operation for Improved Market Reserve Participation			
UC Description	UC focus is on Battery Energy Storage Systems (BESS) performance and reliability in a ESS coupled with a load/PV simulator setup with additional sensors for verification.			
UC Owner	ENELX - Aggregator in Italy			
Data Subject Type	Energy Transmission, Energy Distribution			
Data Subject Description	ENELX - Aggregator in Italy			
Data Source(s)	Battery Management System (BMS) data from BMS data collector BESS data from BESS controller ESS control vectors to the ESS controller Grid services participation reports Power, energy, voltage, frequency related to the grid connection point (grid/ESS meter)			
Data Controller	ENELX - Aggregaor in Italy			
Personal Data	No			
Personal Data Protection Mechanisms	N/A			
Potential Concerns	**Likelihood**	Low	**Impact**	High

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 8 – UC 1: Optimal Management Strategies for Cross-Infrastructure Flexibility Resources to Support Higher RES Shares at the Island Community Level			
UC Description	The UC is about upscaling a preexisting RES & BESS hybrid island microgrid using weather and cross-domain data such as EV and water network data.			
UC Owner	UNIWA - University in Greece			
Data Subject Type	Energy Distribution, Residential Customers, Commercial Customers (tertiary sector)			
Data Subject Description	Smart meter owners (residential & commercial customers on Tilos) RES asset owners / prosumers BESS asset owner			
Data Source(s)	Smart meter data Local & regional control center data Weather station data Wind turbine data PV data BESS data Thermal power station data			
Data Controller	Local energy communities and aggregators			
Personal Data	Yes			
Personal Data Protection Mechanisms	To be considered based on each specific dataset			
Potential Concerns	**Likelihood**	High	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 9 – UC 1: Optimizing and Improving Management and Prediction of DER Production			
UC Description	This UC features a solar demonstration platform and edge-level microservices deployed in public buildings. It aims at asset-level anomaly detection and coordinated flexibility providing using a Virtual Power Plant (VPP).			
UC Owner	ENERC - RES operator in Portugal			
Data Subject Type	Energy Generation, Energy Distribution			
Data Subject Description	DSO in Portugal IPMA - Portuguese national weather institute Weather service providers (UBIMET) DSO Operation and maintenance service providers (including Martim Longo municipality and/or municipality infrastructure service providers)			
Data Source(s)	Energy and power balance dataset (inverter data, grid voltage data etc) Weather and environment data Water distribution, waster management, municipal building data DSO asset inventory list (no real-time data)			
Data Controller	ENERC - RES operator in Portugal			
Personal Data	Yes			
Personal Data Protection Mechanisms	Aggregation (Average production per CPV, periodicity of asset failures)			
Potential Concerns	**Likelihood**	High	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 9 – UC 2: Regional Energy Sector Aggregation Digital Twin			
UC Description	This UC is centered around DaaS by providing data for regional (instead of national) aggregation CO_2 footprint can also be calculated. Main energy sources for the local Distributed Energy Resource (DER) installtion are solar and wind.			
UC Owner	ENERC - RES operator in Portugal			
Data Subject Type	Energy Generation, Energy Distribution, Energy Transmission			
Data Subject Description	DER operators (solar and wind in Portugal) Regional weather service providers			
Data Source(s)	DER generation data Regional weather forecasts			
Data Controller	ENERC - RES operator in Portugal			
Personal Data	No			
Personal Data Protection Mechanisms	N/A			
Potential Concerns	**Likelihood**	Low	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 9 – UC 3: FlexATwin Regional Digital Twin With Multiple Interfaces for Flexibility Across Sectors			
UC Description	The UC is located in a region with the opportunity to aggregate and couple energy sectors such as DER, storage, EVs, municipal buildings.			
UC Owner	ENERC - RES operator in Portugal			
Data Subject Type	Energy Generation, Energy Distribution, Energy Transmission			
Data Subject Description	Relevant EPES stakeholders (generation, DSO, TSO, mobility service provider, aggregators) Weather service providers			
Data Source(s)	Access to data sources from all the relevant stakeholders (generation, DSO, TSO, mobility service provider, aggregators) Weather service data			
Data Controller	ENERC - RES operator in Portugal			
Personal Data	N/A			
Personal Data Protection Mechanisms	N/A			
Potential Concerns	**Likelihood**	Low	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 10 – UC 1: Predictive and Prescriptive Analytics for Improved Energy Performance Certificates Reliability			
UC Description	This UC uses Big Data to improve building EPC reliability by integrating harmonized stakeholder data to implement the EU's 2010 Energy Performance Directive.			
UC Owner	CARTIF - Research Center in Spain VEOLIA - ESCO in Spain			
Data Subject Type	Residential Customers, Industrial Customers			
Data Subject Description	Spanish cadastre authority Smart meter owners Energy system owners			
Data Source(s)	EPC register (Spanish cadastre) EPC databases LiDAR COPERNICUS HEMS/BEMS/DEMS/Open Urban data/Invoices Weather data (historical and forecasts) DEEP, The Curve databases (8000 projects) Smart meter datra (historical and current energy consumption from 973 buildings)			
Data Controller	VEOLIA - ESCO in Spain			
Personal Data	Yes			
Personal Data Protection Mechanisms	For the purpose of the project, it is not expected to use aggredated data. Depending on specific dataset, it will be evaluated anonymization techniques.			
Potential Concerns	**Likelihood**	High	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 11 – UC 1: Weather-enhanced Building Thermal Comfort Prediction to Enable Energy Efficiency Reliable Forecasting			
UC Description	This UC is concerned with enabling energy retrofitting buildings at district level. The main focus lies on the occupant's thermal comfort and related energy efficiency trade-offs.			
UC Owner	AJSCV - Municipal Organization in Spain VEOLIA - ESCO in Spain			
Data Subject Type	Energy Distribution, Residential Customers			
Data Subject Description	AJSCV - Municipal organization in Spain Spanish Cadastre VEOLIA - ESCO in Spain Weather service provider			
Data Source(s)	Water consumption (Excel) LIcense files (AUPAC) Environmental records (AUPAC & Excel) Energy certificates (Excel) Technical construction inspection (Excel) Cadastral data (Excel) Specific tools (i.e. Atlas, SMA, Genweb)			
Data Controller	AJSCV - Municipal Organization in Spain			
Personal Data	N/A			
Personal Data Protection Mechanisms	Even if some data sources can contain personal data, anonymisation techniques will be applied, and however personal data will not be shared within the project.			
Potential Concerns	**Likelihood**	Medium	**Impact**	Medium

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

LSP – UC	LSP 12 – UC 1: De-risking Energy Efficiency Investments			
UC Description	Energy efficiency projects are often fragmented without evidence-based platforms. Big Data Analytics featuring among other datasets building historical financial performance is to close this gap to instill the necessary confidence.			
UC Owner	LEIF - Fund in Latvia			
Data Subject Type	Energy Distribution, Residential Customers			
Data Subject Description	LEIF - Fund in Latvia Weather service provider			
Data Source(s)	CCFI monitoring data EAFI monitoring data Energy efficiency project data (DEEP database, The Curve) Weather service data EPC Invoices			
Data Controller	LEIF - Fund in Latvia			
Personal Data	Yes			
Personal Data Protection Mechanisms	Even if some data sources can contain personal data, personal data will not be shared within the project. Moreover, anonymisation and aggregation techniques will be evaluated for specific dataset.			
Potential Concerns	**Likelihood**	Medium	**Impact**	High

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

5.2 Analysis of potential concerns and countermeasures

Even if yet many use cases are going to be refined with further details, the above section provides many interesting information for the identification of potential concerns and their impacts.

As it emerges from the analysis conducted, at present, operations potentially entailing the processing of personal data are limited only to certain steps of the single LSP/UCs and, in any case, the Partners involved will proceed to the aggregation and/or anonymisation of such data, as the processing of clear data is not necessary for the achievement of the Project objectives.

Figure 3 summarises the classification of the LSP/UCs based on the likelihood of potential concerns, as well as on the level of the impacts. The values of likelihood and impact identify three zones, i.e.: low (blue), medium (gold) and high (orange).

Only 33% of the analysed BD4NRG use cases are in a medium-high zone (orange coloured), and however, for each of them, the consortium is aware of potential concerns and, as it has already clarified, for that reason has yet considered appropriate mechanisms and countermeasures (i.e. aggregation and/or anonymization), for mitigating the risks of potential concerns, or further details will be considered for each specific dataset.

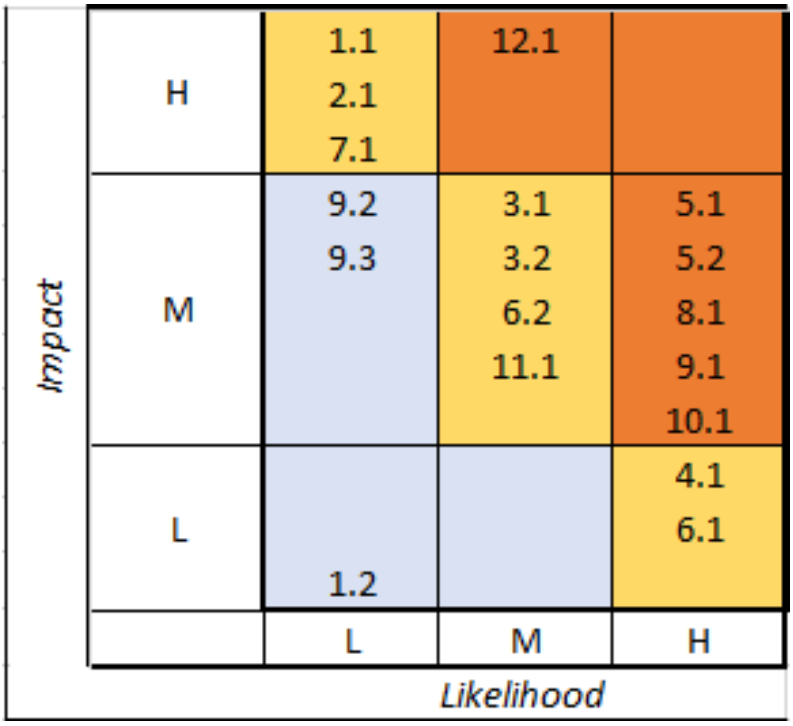

Figure 3 - Analysis of Potential Concerns for BD4NRG LSP/UCs

The methodology, adopted for carrying out this analysis and specification, provides the consortium with a relevant tool and results for monitoring and controlling the use cases during their lifecycle, and consequently this can be repeated periodically for the assessment of use cases.

For this reason, the use case template adopted for the preparation of this specification can be reused as a basis for supporting the assessment of the development activities in BD4NRG. Specifically, the following "assessment checklist" is considered for the next iterations. This checklist represents a simple and valuable tool for a self-assessment of the development activities, and in case of uncertainties, the assessment operator – e.g. LSP/UC owner, component owner – is invited to immediately contact ELEX and the Coordinator. Based on specific concerns and/doubts, ELEX and the Coordinator will identify appropriate countermeasures according to the ethics requirements and the regulatory framework, representing the BD4NRG legal and ethics research protocol.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

Assessment Checklist				
LSP/UC/Component	*<Identifier>*			
Date	*<Assessment Date>*	**Assessment Operator**	*<Identifier>*	
LSP/UC/Component Description	*<Brief description>*			
Data Subject Type	*<Options: {EnergyGeneration, EnergyTransmission, EnergyDistribution, ResidentialCustomer, IndustrialCustomer}>*			
Data Subject Description	*<Short description of the entity from whom or about whom the project collects information in connection with its activities>*			
Data Source(s)	*<List of data source(s)>*			
Data Controller	*<The entity that determines the why (purpose) and the how (terms and conditions) for processing data>*			
Personal Data	*<Options: { Yes / No / NA / Not Sure }>*			
Personal Data Protection Mechanisms	*<If data contain personal data, specifies the purpose and the designed mechanisms to be applied Options: {Anonymisation, Peudonymisation, Aggregation, Minimisation}>* *<In case of uncertainty, please, contact immediately ELEX and Coordinator>*			
Potential Concerns	**Current Likelihood**	*<evaluation performed by the validator>*	**Current Impact**	*<evaluation performed by the validator>*
	Previous Likelihood	*<previous validation score, if any>*	**Current Impact**	*<previous validation score, if any>*

Last but not least, it is important to remark the satisfactory level of awareness on data protection concerns. This can be justified by the frequent presentations of data sharing principles to the consortium since the beginning of the projet and summarised in a presentation containing data protection concerns, countermeasures and principles (see Figure 4).

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

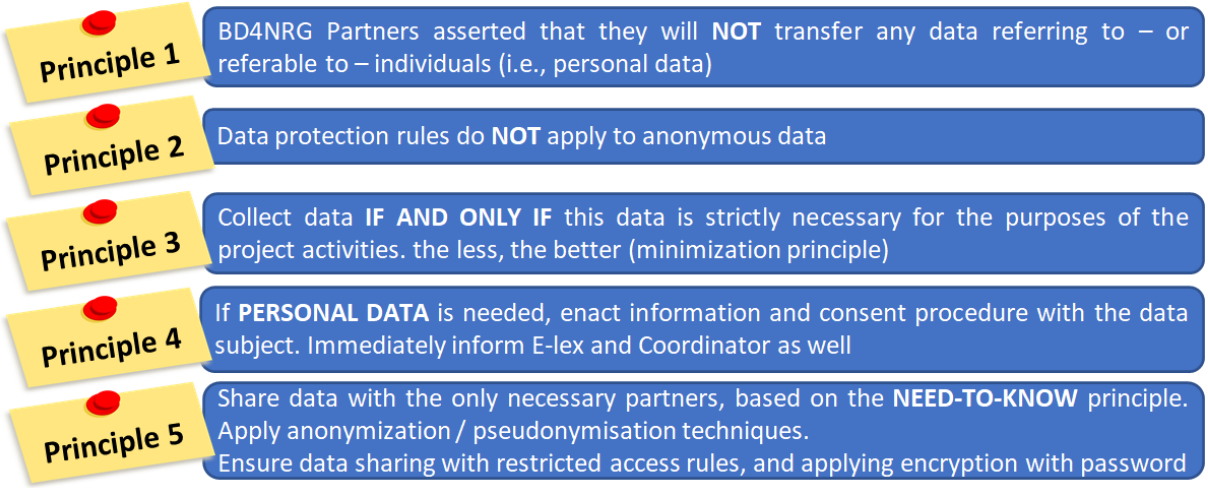

Figure 4 - Data Sharing Principles

These principles are integrated with the last section of this document, where compliance best practices are provided.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

6 BD4NRG compliance best practices

Legal principles and constraints to be taken into account in conceiving and developing the BD4NRG system must ensure the following requirements:

1. **Transparency** and **openness** principles are respected, being transparent about the purpose to use the data; giving appropriate information to individuals to exercise their rights, to data controllers to evaluate their processors, and to Data Protection Authorities to monitor according to responsibilities.

2. Collected personal data is **lawfully** obtained. Lawfulness implies having legitimate grounds for collecting and using the personal data, including having the unambiguously given consent of the individual whose personal data are being processed and not using the data in ways that have unjustified adverse effects on the individuals concerned.

3. Collected personal data is **adequate** and **relevant** to the objectives of the system. For the purpose limitation principle, the collection of personal data must be limited to what is directly relevant and necessary to accomplish the project specified purpose. The purpose has to be legitimate, and it has to be specified and made explicit before collecting personal data.

4. The amount of collected personal data is **proportional** to the objectives of the system. For the data minimization principle, only the minimum amount of personal data which is needed to achieve the specific project purpose must be collected, used and retained. Moreover, data must be adequate and relevant in relation to that purpose.

5. The collected personal data is **accurate**: data has to be the right value, it has to precisely represent the value in consistent form and it must be up-to-date. Procedures to keep data up-to-date are needed.

6. A **storage limitation policy** is defined: personal data must be retained only for as long as is necessary to fulfil the declared purpose. It must be erased or effectively anonymised as soon as it is not anymore needed for the given purpose.

7. Procedures for **granting individual rights** are defined: individuals must have the possibility of effectively and conveniently exercise their rights to access and rectify as well as to block and erase their personal data. Further they have the right to withdraw given consent with effect for the future.

8. **Accountability** principle is respected and technical measures are implemented, in order to be able to demonstrate the compliance with privacy and data protection principles and legal requirements. This means defining clear responsibilities as part of the project research and innovation process, including a partner internal Data Protection Officer. It implies internal audits and handle complaints. A means for demonstrating compliance is the Data Protection Impact Assessment to be carried out by the project, that will be published accordingly with project rules on data confidentiality and EU Commission rules on classified data. It should be noticed that at a national level, accountability is supported by independent Data Protection Authorities for monitoring and checking as supervisory bodies. That's why partners managing personal data have to follow the internal procedure outlined in the DoA's section 5 including notification (if it is the case) to the national authorizing authority. At IT system level, examples of accountability measures are related to tracking of personal data access and of communications with external systems.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

9. Appropriate measures for **data security** are implemented: information security addresses integrity, confidentiality and availability concerns. They are important also from a privacy and data protection perspective, requiring a set of rules to be applied to limit access to personal data only to authorized people, and to ensure that the data is trustworthy and accurate. Therefore, data should be kept secure applying Privacy Enhancing Technologies, preventing accidental disclosure of personal data, securing communications with external stakeholders (such as for instance external systems).

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

7 Conclusions

This document provides the reader with a detailed analysis of the legal and security framework to be applied in the context of BD4NRG, based on relevant references, i.e. NISD, GDPR, Third Energy Package, and the Electricity Network Codes and Guidelines. This conceptual framework lays the foundation for respecting fundamental requirements, dealing with privacy, data protection and security.

The document provides a methodology for the identification of potential concerns within the twelve Large Scale Pilots and their use case scenarios, as well as for their assessment in terms of likelihood and impact.

A template for gathering data and performing self-assessment has been defined and it has allowed to obtain a preliminary level of risks associated to a set of 18 high priority and/or mature use cases within the 12 Large Scale Pilots.

Currently, only 6 (33%) of these use cases are positioned in a medium-high zone, and so these will be particularly monitored and controlled. This analysis will be periodically repeated, by using the assessment checklist identified in this document, in order to check trends and improvements during the project lifecycle, and it will be evaluated how the consortium will fit the requirements in the LSP implementation, as well as will enact appropriate countermeasures for ensuring privacy, data protection and security.

Last but not least, the analysis performed in this task remarks how a satisfactory level of awareness of the consortium on these concerns can be achieved by frequently presenting principles and guidelines, as distilled documents (e.g. short presentations), and by clarifying key concepts coming from the legal framework, e.g. during one-to-one conference calls or focused webinars.

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.

8 References

[1] Hancher, L., Kehoe, A.-M., & Rumpf, J. (2020, January). The EU Electricity Network Codes and Guidelines: A Legal Perspective. https://cadmus.eui.eu/bitstream/handle/1814/66431/RSC_FSR_RR_2020.pdf

[2] Regulation (EU) 2016/679 (2016, April). General Data Protection Regulation (GDPR). https://eurlex.europa.eu/eli/reg/2016/679/oj

[3] Smart Grid Task Force 2012-14. (2014, March). Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems. https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

[4] European Smart Grids Task Force. (2016, November). My Energy Data. https://ec.europa.eu/energy/sites/ener/files/documents/report_final_eg1_my_energy_data_15_november_2016.pdf

[5] Directive EU 2016/1148. (2016, July). Security of network and information systems ("NIS Directive" or "NISD"). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

[6] Directive EU 2015/1535. (2015, September). Procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535

[7] European Parliament. Briefing The NIS2 Directive. (2021, February). https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[8] Proposal for NIS2 Directive. (2020, December). https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF

BD4NRG project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 872613.