The BRIGHT project is co-founded by the EU's Horizon 2020 innovation programme under grant agreement No 957816

Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design

Deliverable D2.2 Privacy, Ethics and Legal Requirements

Author(s): Andrea Iannone (CEL), Piercosma Bisconti Lucidi (CEL), Riccardo Santilli (CEL), Carmela Occhipinti (CEL), Vjekoslav Delimar (ISKRA), Tomaž Dostal (ISKRA), Gabriela Bodea (TNO), Giuseppe Raveduto (ENG)

The project Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design (BRIGHT) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957816. The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the Innovation and Networks Executive Agency (INEA) or the European Commission (EC). INEA or the EC are not responsible for any use that may be made of the information contained therein.

Imprint

Title:	Privacy, Ethics and Legal Requirements
Contractual Date of Delivery to the EC:	31.07.2021
Actual Date of Delivery to the EC:	30.07.2021
Author(s):	Andrea Iannone (CEL), Piercosma Bisconti Lucidi (CEL), Riccardo Santilli (CEL), Carmela Occhipinti (CEL), Vjekoslav Delimar (ISKRA), Tomaž Dostal (ISKRA), Gabriela Bodea (TNO), Giuseppe Raveduto (ENG)
Participant(s):	CEL, COM, ENG, TNO, ISKRA
Project:	Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design (BRIGHT)
Work Package:	WP2 – BRIGHT Technology and Novel Multi-Value Service Design
Task:	T2.4 – Privacy, Ethics and Legal Compliance Framework
Confidentiality:	Public
Version:	1.0

Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

Table 1 - List of Acronyms and Abbreviations

BRIGHT	Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design
CO_2	Carbon dioxide
DR	Demand-Response
DSO	Distribution System Operators
ER	Ethics Requirement
EDC	Error Detecting Code
ESG	Environmental, Social, and Governance (indicators)
FE	Framework element
GDPR	General Data Protection Regulation
gr	grams
kW	kiloWatt
kWh	kiloWatt hour
LEC	Local Energy Community
LR	Legal Requirement
ML	Machine Learning
P2P	Peer-to-peer (technology)
PELR	Privacy, Ethics, and Legal Requirement
PMR	Privacy Macrorequirement
PSR	Privacy Subrequirement
PV	Photovoltaic
SAT	Social Acceptance of Technology (method)
SDG	Sustainable Development Goal
SGAM	Smart Grid Architecture Model
SMR	Cybersecurity Macrorequirement
SR	Standards Requirement
SSR	Cybersecurity Subrequirement
WP29	Working Party 29

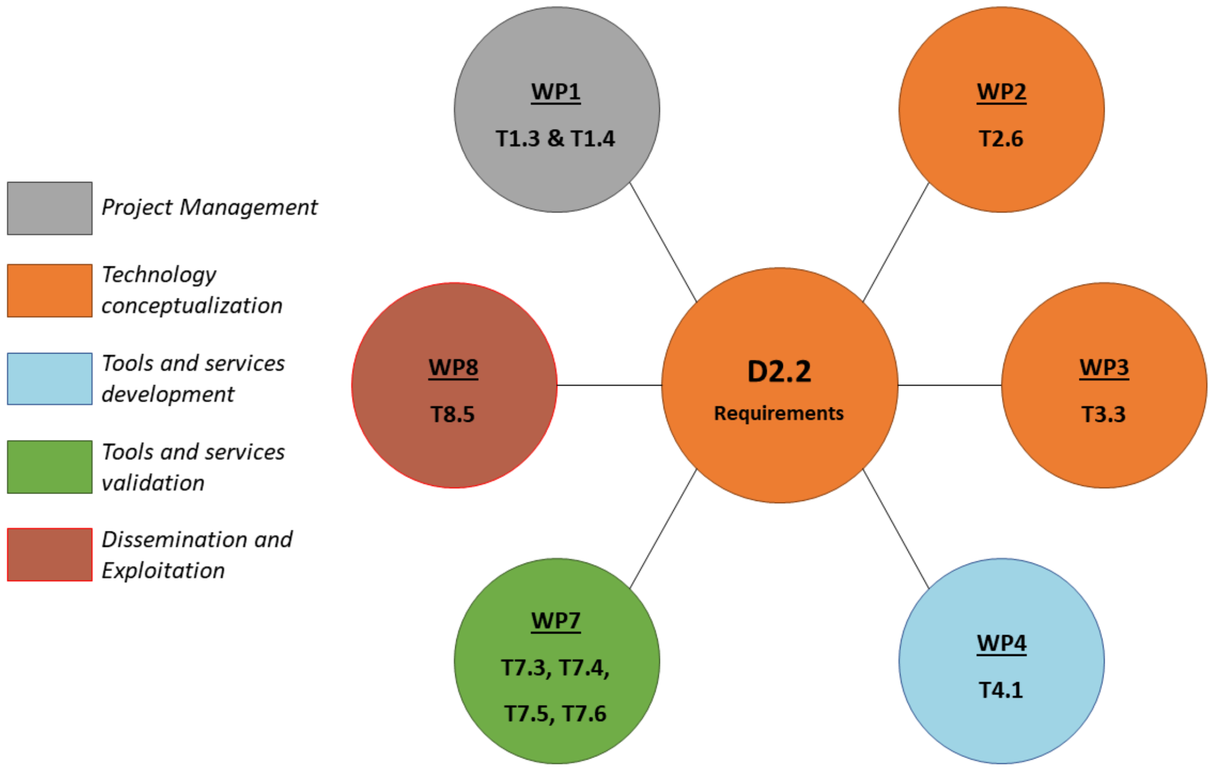
Executive Summary

The goal of this deliverable was to put forward, for the BRIGHT project as a whole, requirements related to Privacy, Cybersecurity, Ethics, and Legal dimensions to add to the requirements generated in WP10. The goal has been achieved by applying an approach that consisted in extrapolating said requirements from a review of the existing legal, normative, and disciplinary frameworks. For each of the four dimensions, the outcome has been as follows:

- Privacy – compliance with GDPR is of paramount importance, not difficult to ensure, and safeguards individuals' fundamental rights.
- Cybersecurity – under the EU legal framework and considering the state of the art, rules and policies have been put forth that mitigate or avoid risks and favour the obtainment of system integrity, accountability, and confidentiality.
- Ethics – three main branches of ethics (deonthological, utilitarian, and virtue) have been applied to BRIGHT as a whole and served to extract requirements regarding the technological, environmental, governance, and social aspects of the project.
- Legal – standards and legislative packages were analysed to distil four requirements.

All consortium partners will benefit from the experience of adhering to these requirements by either acquiring knowledge that aids in avoiding or mitigating specific concerns or in crafting a virtuous and substantiated offering to future consumers, citizens, and communities. The present deliverable, in fact, has multiple ramifications throughout the entire project (as shown in Figure 1) and is a central piece in the strategy the project has instantiated for achieving its objective of bringing DR closer to European consumers.

Figure 1 - The connection of D2.2 to other BRIGHT project activities


Project Management
Technology conceptualization
Tools and services development
Tools and services validation
Dissemination and Exploitation
WP1
T1.3 & T1.4
WP2
T2.6
WP8
T8.5
D2.2
Requirements
WP3
T3.3
WP7
T7.3, T7.4, T7.5, T7.6
WP4
T4.1

1 Introduction

This deliverable aims to identify the relevant requirements for the BRIGHT project as a whole with respect to the four key dimensions of privacy, cybersecurity, ethics, and law. Overall, the approach adopted has been to base the requirement on an analysis of these dimensions' state of the art as represented by existing regulatory frameworks and disciplinary condition. More specifically, the approach to each dimension, which correspond to the four main sections of this deliverable, was as follows:

- The privacy dimension focuses on data protection requirements as defined both by the technical state of the art and the GDPR, which has been analysed separately from other regulations given its importance with respect to individuals' fundamental rights as opposed to norming a specific aspect of a market or sector.
- The cybersecurity dimension identified the energy grid as a critical infrastructure, and therefore both subject to existing legislative and a potential beneficiary of state-of-the-art measures.
- The ethics dimension offered an opportunity to advance positive requirements related to technology, environmental, social, and governance aspects that could risk to be overshadowed by managerial considerations of energy grids.
- The legal dimension provides requirements based on an overview of European regulations, directives, and standards pertaining to energy markets, energy communities, and DR.

The requirements provided in each of these sections are relevant to BRIGHT consortium partners because they are reflect the normative and social zeitgeist within which consumers, citizens, and communities will orient their choices to adopt or reject DR technologies, services, and products, especially given that BRIGHT will implement AI algorithms at large scale in an attempt to maximize the effectiveness of DR. Without demonstrating adherence to the requirements, the BRIGHT project could incur in a broad set of risks with mild to severe impact. Some risks could derive from the project's use of AI algorithms at vast scale to reach its objective of maximizing the effectiveness of DR. These risks are differentiated and addressed in Sections 2 and 0.

Section 2 examines GDPR in order to extract PSRs. Cybersecurity requirements are detailed in Section 3. Section 0 provides an overview of ethics branches in order to apply the most apt ones to the BRIGHT project. Subsequently, the section puts forward requirements related to technologies (some of which harken back to PRs) and to environmental, social, and governance aspects connected to the management of flexibility trading systems such as those that BRIGHT is developing. Finally, Section 5 is divided into two main parts. The first reviews some standards and certifications applicable to the project's technologies, particularly those used in smart metering devices to ensure safety, accuracy, and communication compatibility of device-to-cash systems. The second examines the texts of relevant regulations and directives for the benefit of the consortium and other similar projects. A full list of requirements is provided in Annex 1 – Full list of BRIGHT Privacy, Ethics, and Legal Requirements.

2 Privacy and data protection

The results and the outcomes of the BRIGHT Project might impact (either positively or negatively) some of the fundamental rights recognised at EU and national level within the Member States.

In particular, considering that the Project deals with critical infrastructure such as the energy one and with the implementation of smart meters in the users' houses, it appears necessary to preliminarily analyse privacy and data protection as fundamental rights, as they have been defined within EU and Members States' legislation. Consequently, the protection of privacy and personal rights becomes a specific legal requirement that the Project must comply with, during the Project itself, but also in terms of outcomes.

In the present section, after an introduction on privacy and data protection as fundamental rights, we will be briefly recall the principles of the GDPR identified as "privacy requirements" that will be satisfied by the implemented IT solutions, having regard also to the provisions set forth within the EU Directive 2019/944 (the "**Electricity Directive**", see Section 5.2.1). Section 0, instead, will deal with the ethics requirements of BRIGHT.

2.1 Privacy and data protection legal framework

The identification of the privacy and data protection requirements whose compliance will characterize the BRIGHT Project during its life, as well as its outcomes, should start considering the following.

First, the smart meters implemented in the BRIGHT project belong to complex IT infrastructures that, to properly function, require not only the collection and analysis of data, but also the exchange of that data with other IT infrastructures (and ultimately with competent and responsible individuals appointed to monitor and potentially intervene on it). In this respect, considering the source (i.e. households, electric vehicle power grids, etc.) from which such data will be gathered/collected/extracted, it is possible those data include personal information, i.e. personal data[1], in the information exchange cycle. These data might be analysed through AI algorithms: the ethical implications of the use of AI systems, and the legal implications with regard to the recent EU proposal (*Proposal for a Regulation on a European Approach for Artificial Intelligence*, 2021), will be discussed in Section 4.3. Having assumed as much, it should also be considered that the main objective of BRIGHT is to implement a DR technology in order to maximize the efficiency of the energy distribution infrastructure. The efficency of the DR mechanism is highly dependent on the quality and quantity of data collected by the smart meters in the households. Therefore, it is necessary that the BRIGHT Project performs a balancing operation among two (apparently) conflicting interests: privacy and data protection from one side, and efficient collection of exploitable data on the other side.

To sum up some conceptual differentiations, we can say that privacy (even if there is not a generally accepted definition) can be considered as providing for a general prohibition of interference in the private life of an individual (with of course, certain limitations). On the other hand, the protection of personal data, can be instead intended as a complete system of rights, to be balanced and to be exercised and activated only when personal data, i.e. information that can identify (directly or indirectly) a person, are processed. This means also that data protection rules and requirements

[1] Pursuant to article 4 (1) of GDPR, personal data is defined 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*".

shall be complied with even when the processing operation having as object personal data do not interfere with the privacy of the individual.

Having in mind this introduction, and the scope and the objectives of the Project, it is now necessary to focus the attention on the legislative requirements in terms of data protection adopted at EU level. As it is notorious, the first legislative instruments that was issued by the EU to regulate this subject matter was Directive 95/46/EC. However, in consideration to the technological development as well as having regard to the legislative instruments used (a directive, which leave a certain margin of discretion to Member States in implementing it) in 2018 was issued the EU General Data Protection Regulation no. 2016/679 (hereinafter "**GDPR**").

As of today, GDPR is the most relevant EU legislative source in terms of providing those rules and principles that should be respected when, upon the occurrence of certain conditions, personal data are processed.

For the purpose of the present document, here it is worth to recall that the compliance with GDPR in practical terms entails not only the respect of the principles set forth in of that piece of legislation, but also the capacity of an individual (a data subject) to exercise his/her rights.

In addition, special attention should be paid to the interrelation between GDPR and the so-called Electricity Directive (*Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on Common Rules for the Internal Market for Electricity and Amending Directive 2012/27/EU*, n.d.), which is part of the legislative package named "Clean Energy for All Europeans"[2] and specifically regulates smart meters' deployment. For details on standards regulating smart meters, see Section 5.1; for more details on said directive and the package as a whole, see Section 5.2.1.

In particular, the Electricity Directive provides for a general obligation for the Member States to regulate smart metering without incurring in discrimination of consumers (which is as well as ensuring the protection of their personal data). For the sake of clarity, it should be noted that even if the Electricity Directive is a directive (i.e. one of the EU legislative acts listed in article 288 TFEU), and therefore it is not directly applicable in the Member States, but rather it has to be timely transposed into national legislation, it can in any case provides some guidance in identifying privacy and data protection requirements specifically targeted in smart metering and smart grid.

Figure 2 - Clean Energy for All Europeans package

In this respect, it is interesting to see how article 20, paragraph 1, letter f) of the Electricity Directive essentially represents a transposition of the general duty of transparency provided in articles 5, 12, and 14 of GDPR as well as article 20, paragraph 1, letter e) recognized also the importance of implementing mechanism in data exchange enabling for the consumer/data subject to exercise his/her rights of access as provided in article 15 of GDPR. As last remark, in a very general term, and therefore with a very broad meaning, article 23, paragraph 3 of the Electricity Directive concerning "Data management" provides that "*The processing of personal data within the framework of this Directive shall be carried out in accordance with Regulation (EU) 2016/679*".

[2] https://ec.europa.eu/energy/topics/energy-strategy/clean-energy-all-europeans_en

2.2 Privacy and data protection requirements

To define privacy and data protection requirements, we evaluated whether the project or its results would include personal data in WP10. In consideration of positive answers to this question, some steps have been taken in order to protect the personal data of the individuals that might be affected. **Documents supplied within the confines of WP10 guarantee the Privacy and data protection macrorequirement: compliance with GDPR.** In addition, Table 2 summarizes Privacy and Data Protection subrequirements.

Table 2 - Privacy and Data Protection requirements

#ID	Requirements	Description
PRS1	Transparency	The **purposes of the data processing** should appear clear and intelligible for the data subject. This can be ensured providing all the appropriate and necessary information to data subjects to exercise their rights, to data controllers to evaluate their processors, and to Data Protection Authorities to monitor according to responsibilities. Thus, the technology solutions and their relative data models should ensure that a data subject may get access easily, at any time after the start of the data processing operations, to the information processed. When accessed, the information and the way it was processed should both be clear and intelligible.
PSR2	Lawful data collection	The data processing shall originate from those personal data that have been collected with a lawful ground. Particular attention should be paid when implementing those components that will help to collect and get the **data subject's consent**. In this respect, the relevant implementer should ensure the possibility to map the data flow. Particular attention should be given in case of secondary processing (even if, at the time of submission, this kind of operations are not foreseen).
PSR3	Personal data collected are (i) adequate, (ii) proportionate and (iii) relevant to the objectives of the system	The implementation of the principle of **purpose limitation and data minimisation**, representing two of the core principles set forth in GDPR, requires that the type and the amount of data collected shall be proportionate to the purposes to be achieved, and at the same time, the purpose itself shall be legitimate. In this respect, data should be gathered if and only if it is strictly necessary for achieving the specified purpose and that data is "**need to know**".
PSR4	The personal data collected are accurate	Besides the amount and the relevancy of the data collected, the technology solutions should ensure that the data to be processed are **accurate**, i.e. procedures to keep data are correct and up-to-date in all details are needed.
PSR5	Storage limitation	The development team of the technology solutions should define and implement an infrastructure pursuant to which it is possible to foresee for how long the personal data will be stored (ideally **the shorter the better**), and that in any case shall be compliant with the applicable legislation. Data subjects must be informed about it. Moreover, provided that those data are no longer necessary to fulfil the said scope, and any other restrictions can be found applicable, such data should be immediately erased and/or anonymised pursuant to the best standards and practices.
PSR6	Procedures for granting individual rights	The components of the technology solutions should be designed taking also into consideration how, in concrete, the relevant data subject might exercise his/her rights in connection with the data processing. In this respect, the relevant implementer should be aware of all the rights that GDPR grants to data subjects, and for each of them tailor **a specific solution** (e.g. data subjects have the right to rectify their data and to request their erasure). It should be also taken into account mechanisms for influencing or stopping the data processing fully or partially, manually overturning an automated decision, data portability precautions to prevent lock-in at a data processor, breaking glass policies, single points of contact for individuals' intervention requests, switches for users to change a setting (e.g. changing to a nonpersonalised, empty-profile configuration), or deactivating an auto pilot or a monitoring system for some time. Issues regarding blockchain compliance with GDPR are discussed in the next section.

PSR7	Accountability principle and technical implementation	The implementation of the accountability principle entails that the technology solutions should allow a clear **identification of the responsibilities** related to the data processing. In particular, examples of accountability measures are related to **tracking** of personal data access and of communications with external systems. Transparency is a prerequisite for accountability. Mechanisms for achieving or supporting transparency comprise logging and reporting, an understandable documentation covering technology, organisation, responsibilities, the source code, privacy policies, notifications, information of and communication with the persons whose data are being processed. Transparency ensures that all privacy-relevant data processing including the legal, technical and organisational setting can be understood and reconstructed at any time (*Privacy and Data Protection by Design*, 2015).
PSR8	Appropriate data security measures	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 should be implemented. 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). Integrity, confidentiality and availability of data should be granted.
PSR9	Data unlinkability	Unlinkability ensures that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context, and that means that processes have to be operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy relevant data outside of the domain. Unlinkability is related to the principles of necessity and data minimisation as well as purpose binding. Mechanisms to achieve or support unlinkability comprise of data avoidance, separation of contexts (physical separation, encryption, usage of different identifiers, access control), anonymisation and pseudonymisation, and early erasure or data. (*Privacy and Data Protection by Design*, 2015)

2.3 Privacy and data protection requirements as multi-dimensional risk mitigation and avoidance factors

In general terms, it is possible to say that the main privacy concern regards a general dis-respect of the principles expressed above. Also considering that DR and smart meters are complex technology solutions that have been developed to increase the efficiency and the effectiveness of the electric supply chain. Moreover, considering the scope pursued by the implementation of smart grid it is possible to say that:

“Smart grids improve electricity generation and distribution through optimization and projection of electricity consumption by leveraging communication networks to exchange information between those different parties” (Butun et al., 2020).

In particular, smart grid can be seen as a complex of five domains (according to the Smart Grid Architecture Model - SGAM): generation, transmission, distribution, distributed energy resources and customer premises (consumption). Each domain poses questions in terms of privacy and data protection (as well as ethics, security and other social concerns addressed in the following chapters). Indeed, to properly functioning, each domain requires a considerable amount of data, entailing the exchange of such data Distributor System Operators (hereinafter “**DSO**”) and aggregators, prosumers, and consumers.

In terms of “privacy concerns”, among the other, the following might be identified as the main (general) ones:

- the possibility of inferring relevant information (e.g. particular habits) from personal data, due to the collection and processing of great amount of data and personal data;
- metering data will be accessible by several independent actors (e.g. DSO, service provider, the consumer) (*Smart Grid Security: Recommendations for Europe and Member States*, n.d.) performing roles as data controllers, data processors, third parties, recipients etc.;

- effective exercise of consumer/data subject's rights.

Another important concern to be addressed regards the compliance of the blockchain technology implemented in BRIGHT with the GDPR. The GDPR compliance of blockchain is debated. Nevertheless, limited scientific literature is facing up the issue systematically and, therefore, further understanding is crucial. Many scholars point out some difficulties for the blockchain in order to be compliant with the GDPR. Here we will list some of these open issues, mainly taken from Sim et al. (Sim et al., 2019).

The most problematic point is the Article 17 "*right to erasure*": the blockchain, in order to be tamper-resistant, is also immutable, and therefore does not allow information to be deleted. This is also highlighted by Hristov & Dimitrov (Hristov & Dimitrov, 2018) as a backbone of blockchain GDPR compliance. For the same reason, the right of rectification (Article 16) seems to be hardly implementable since no modification can be done to a block after it is added. If a block is modified, in fact, it would alter the entire chain since the hash of the following block would no longer point to the preceding one.

In BRIGHT, blockchain is not used for storing data classified as personal data. Instead, blockchain is used as an additional layer that provides data integrity and auditability features. Data classified as personal data are stored in traditional databases (off-chain) whereas blockchain is only used to store the hash of that data (in-chain) as a proof of integrity of data itself.

It is also difficult to define the "data controller" (Article 4), since any chain is replicated in each and every register, as required by P2P technologies. On the side of data minimization, the blockchain goes against Article 25 since the data are not stored only between the participants involved in a transaction but replicated throughout the nodes.

Another urgent problem regards the anonymization/pseudonymization of personal data on the blockchain. GDPR does not apply to anonymized data but does apply to pseudonymized data. The problem is therefore to understand if hash identifiers on the blockchain should be considered anonymized or pseudonymized data. WP29 and the French Data Protection Authority (CNIL) seem to agree on the fact that these data *are* pseudonymized and therefore GDPR applies. CNIL issued the following statement[3]:

"The very architecture of blockchains means that these identifiers are always visible, as they are essential for its proper functioning. The CNIL EBSI GDPR Assessment 14 therefore considers that this data cannot be further minimised and that their retention periods are, by essence, in line with the blockchain's duration of existence"

Similarly, the WP29 states that: "If the range of input values the hash function are known they can be replayed through the hash function in order to derive the correct value for a particular record. For instance, if a dataset was pseudonymised by hashing the national identification number, then this can be derived simply by hashing all possible input values and comparing the result with those values in the dataset." (*Article 29 Working Party Opinion on Anonymisation Techniques*, 2014)

Lastly, the EU Blockchain Observatory and Forum (2018) states that the problem of the pseudonymity or anonymity of hashing is still a grey area:

"*Hashing is at the heart of many of the most important properties of blockchains, providing much of the 'magic' of decentralisation. This question of whether hashed personal data should be considered personal data is hotly debated at present, and unfortunately much of this debate relies on rather complex details. Also, it should be kept in mind that not all hashing algorithms are equal and that the most advanced algorithms should always be preferred. As stated above, these issues have not been conclusively settled by the data protection authorities, the EDPB or in court. At this stage, a*

[3] https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

desirable outcome of the debate regarding the status of hashed personal data could be: it depends. the gist of it could potentially come down to the question of identifying potential reversibility or linkability risks".

Last point on GDPR, another issue involving personal data is the so-called "linkability risk" (*The EU Blockchain Observatory and Forum*, 2018):

"*Linkability risk, or the risk that it is possible to link encrypted data to an individual by examining patterns of usage or context, or by comparison to other pieces of information*".

Since the concrete use of the blockchain in BRIGHT is today not technically fully clarified, is not possible to further assess the compliance of BRIGHT's blockchain with the GDPR. Though, the concerns discussed above should be taken in serious considerations during the technical development of BRIGHT's blockchain in order to, possibly, ensure that the data on the blockchain can be considered anonymized and not pseudonymized, so that GDPR simply does not apply.

In the table below we summarize the potential concerns or threats impacting BRIGHT project.

Table 3 - Potential Concerns or Threats impacting Privacy and Data Protection Requirements

# ID	Requirement	Potential Concerns or Threats
PSR1	Transparency	● PTHR1 – Data Subject is not informed of (i) which data are collected; (ii) which is the source of the collection; (iii) who are the actors involved in the collection and subsequent processing; and (iv) the purposes of the data processing. ● PTHR2 – Data processing is done for different purposes from the ones agreed with the data subject.
PSR2	Lawful data collection	● PTHR3 – Data Subject is not aware of data collected and shared. ● PTHR4 – The collection of data is made on a wrong legal basis or in absence of a legal basis.
PSR3	Personal data collected are (i) adequate, (ii) proportionate and (iii) relevant to the objectives of the system	PTHR5 – It is quite frequent the collection of unneeded (personal) data, i.e. data not relevant to the objectives of the system and for the agreed purposes of data processing.
PSR4	The personal data collected are accurate	PTHR6 – Lack of information among involved parties is the primary potential cause for inaccurate data in a system.
PSR5	Storage limitation	PTHR7 – If data is stored for longer than the necessary time period, then there is an increased chance of that data being tampered with.
PSR6	Procedures for granting individual rights	PTHR8 – Lack of information of the data subject rights at design phase impacts on enabling/disabling the exercise of individual rights themselves.
PSR7	Accountability principle and technical implementation	PTHR9 – Accountability of the system is impacted by the lack of provenance information regarding activities of the components (i.e. logs), access to the system, integrity of data collected, integrity of data exchanged.
PSR8	Appropriate security measures	PTHR10 – In some cases, data stored on the blockchain might be used as a basis for inferences that violate individual's fundamental right to privacy.
PSR9	Data unlinkability	PTHR11 – Security measures are not at the state of the art or are not up-to-date

3 Cybersecurity

This section provides an overview of applicable EU-wide legislation and of the state-of-the-art reference architecture model for smart grids (SGAM). The requirements that can be found in Section 3.1.3 are also envisioned to be consumer-friendly, in the sense that they consider how residential consumers have smart meters in their home, which need to be guarded against malevolent intent of cybercriminals.

3.1.1 Cybersecurity legal framework

The analysis of the legislative requirements imposed at EU level in terms of (cyber) security aspects is particularly relevant in consideration to fact that the Project deals with critical infrastructure, that can be defined as "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*"[4]. The definition most certainly applies to the BRIGHT technology infrastructure, as it connects EU citizens to energy, a resource vital for their well-being.

3.1.1.1 NIS Directive

As already recognised in 2012 by ENISA, the impacts of cyber-attacks and threats on smart grid and smart metering infrastructures might affect society's way of life. It is for this reason that in the next paragraphs the European cyber-security legal framework will be analysed. From this analysis, it will be possible to infer those security requirements that the Project intends to implement within the components of the BRIGHT architecture.

At the EU level in 2013, the "Cybersecurity Strategy of the European Union – an Open, Safe and Secure Cyberspace" (hereinafter, the "**Strategy**") (*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013) was launched. Among the five objectives identified by the Strategy there was also the so called "cyber-resilience", to support the internal market (NIS Directive, Article 1) and also to boost the security of the EU.

Already within the Strategy the EU was promoting the adoption of a more uniform legislative approach to tackle cybersecurity threats, in particular with reference to those having cross-border dimension.

It is in this light that the adoption of the Directive on Security of Network Information System EU 2016/1148 (hereinafter the "**NIS Directive**") should be read and welcomed. The NIS Directive is the first horizontal piece of legislation aimed at protecting the security of network and information systems.

In particular, the NIS Directive has 3 main objectives:

1. to improve national cybersecurity capabilities;
2. to build and foster cooperation (on cybersecurity) at the EU level; and
3. to promote a culture of risk management and incidents reporting among key economic actors, operators providing essential services for the maintenance of economic and societal activities, and digital service providers.

[4] Article 2, letter a) of the COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

The NIS Directive sets forth obligations directly on Member States, who have a duty to transpose into national legislation the said directive, providing for specific obligations on operators of essential services[5]. The actors involved in the production and transmission of electricity and heat are clearly operators of essential services and, therefore, shall be considered as the addressees of the obligations set forth by the NIS Directive. In fact, reading in conjunction article 4(4) and article 5(2) of the NIS Directive, an organization can be defined as an "operator of essential services" (hereinafter "**OEP**") provided that:

- it is a public or private entity of the type referred in Annex II of the NIS Directive, which includes energy (including electricity), transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure. In this respect, it is worth noticing that being the NIS Directive a directive pursuant to article 288 of the TFEU, during it transposition into national legislation, it might be subject to certain changes. With reference to the identification of the operators of essential services, even if the said legislation provided the main criteria, however by 2018 Member States had to identify the operators of essential services with an establishment on their territory;
- the said entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems;
- an incident would have significant disruptive effects on the provision of that service.

The obligations created by the NIS Directive can be divided in two macro-categories:

a) security requirements
b) information/notification obligations.

It is important to remark that the NIS Directive and GDPR cannot be seen as alternatives, as they do not have the same subject matter. This means that, in terms of compliance, the Project shall have to bear in mind both pieces of legislations, as well as proposing and implementing IT requirements and components able to satisfy both.
In terms of ensuring the security of the network and of the information system as defined in article 4 (2), the NIS Directive provides that Member States shall ensure that OEPs shall adopt:

- appropriate and proportionate technical and organisational measures with regard to the security of the network and information systems they use in the provision of their services;
- these measures shall aim to: (i) manage the risks posed to those systems and (ii) prevent and minimise the impact of incidents affecting those systems, with a view to ensuring the continuity of their services; and
- shall have regard to the state of the art and ensure a level of security appropriate to the risk posed.[6]

[5] For the sake of completeness, the NIS Directive provides obligations to be complied with by service operators (cloud computing services, online marketplaces and search engines), for which a dedicate implementing regulation providing for more details was in 2018.

[6] Articles 14 (1) and (2) and 16 (1) and (2) of the NIS Directive.

In this respect, it should be noted that, since there is not further explanation on the concepts of proportionality and appropriateness in relation to such measures, a large discretion has been left to Member States.

Nevertheless, a risk-based approach shall always be born in mind when identifying and implementing such measures and should be considered a sort of guiding light when implementing security measures. In this respect, in order to give more content to the "risk approach" suggested, a useful reading is represented by the ENISA document "Appropriate security measures for Smart Grid" (*Appropriate Security Measures for Smart Grids Guidelines to Assess the Sophistication of Security Measures Implementation*, 2012), whereby, inter alia, it is provided that the risk assessment shall be performed during the entire life cycle of the smart grid itself (and so also during the creation of the same), and in particular, the risk assessment "*is a key preliminary step that should be conducted in order to understand what risk level is appropriate/acceptable for each organisation before deciding upon the required sophistication levels needed by the smart grid organization*." (*Appropriate Security Measures for Smart Grids Guidelines to Assess the Sophistication of Security Measures Implementation*, pp. 15-16, 2012).

Moreover, in order to foster the homogeneity of these security measures, the NIS Cooperation Group in 2018 published some guidelines whereby the following principles were identified and explained in order to give some guidance: "*these measures should be effective, tailored, compatible, proportionate, concrete, verifiable and inclusive*" (*Reference Document on Security Measures for Operators of Essential Services*, 2018).

In addition, in the same document, the NIS Cooperation Group identifies the following 3 macro–areas (each of them sub-categorized) in which specific security policies should be implemented (see Table 4).

Table 4 - NIS Cooperation Group macro-area

Macro - area	Sub - category
Governance and Ecosystem	Information System Security Governance & Risk Management
	Ecosystem management
Protection	IT Security Architecture
	IT Security Administration
	Identity and Access management
	IT Security maintenance
	Physical and environmental security
Defense	Detection
	Computer security incident management

Compliance with this set of obligations can be distinguished in obligations to (i) notify the national legislator/regulators concerning incidents that met a certain threshold and (ii) voluntarily[7] disclose information/incidents. (Michel & Walden, 2018).

For the purpose of the present deliverable, what it is relevant is "the incident notification obligation". In particular the NIS Directive defines an incident as "*any event having an actual adverse effect on the security of network and information systems*". In order to determine the significance

[7] Which, according to the NIS Cooperation Group Guidelines on notification of Operators of Essential Services incidents – Formats and procedures" publication 05/2018, can allow authorities to get a better situational awareness as well as to identify potential new threats and consequently informs also other OES.

of the impact of an incident, operators of essential services and digital service providers must take into account the following parameters:

1. the number of users affected by the disruption of the essential service;
2. the duration of the incident; and
3. the geographical spread with regard to the area affected by the incident.

The timing of the notification will have to take place without unjustified delay. As per the security measures, also in this case the NIS Cooperation Group published some useful guidelines in 2018, aimed at providing non-binding technical guidance "*to national competent authorities and CSIRTs with regard to formats and procedures for the notification of incidents by OES, to facilitate alignment in the implementation of the NIS Directive across the EU*". (*Guidelines on Notification of Operators of Essential Services Incidents – Formats and Procedures*, 2018). Indeed also in this case the adoption of uniform guidelines could represent a vital asset to tackle cross-border incidents, improve collaboration and the aggregation of the data and their analysis, as well as improve the entire efficiency of the system.

In terms of notification procedures, the NIS Cooperation Group provides the following (*Guidelines on Notification of Operators of Essential Services Incidents – Formats and Procedures*, 2018):

- alert notifications to be addressed to the competent national authority or to the competent Computer Security Incident Response Team (hereinafter "**CSIRT**") in order to:
  - "*Offer support to the affected organization, for example, the CSIRT could give technical support.*
  - *Assess the potential impact for essential services, citizens, the society, the economy, etc.*
  - *Inform, in exceptional circumstances, and when this is in the public interest, other organizations, so they can take action.*
  - *Prevent spreading or reduce the impact by warning and sharing information with relevant organizations, for example with other OESs, CSIRTs, etc.*
  - *Inform authorities abroad when there is significant impact across the EU*".
- Follow up notifications to update on the status of the alert notification.

In addition, the documents then highlights how much is important the timing of the notification itself, proposing also different methods to transmit the same, as well as indicating that the same notifications shall be also protected.

3.1.1.2 Cybersecurity Act

The Cybersecurity Act (*REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 52*, n.d.) was adopted in April 2019 and, among its objectives, it introduced the first EU certification scheme for ICT digital products, services, and processes. In this respect, it should be noted that the certification scheme is based on a risk-based approach.

Moreover, a European Cybersecurity Certification Group was established in order to favour the implementation of the certification framework.

3.1.2 Cybersecurity technical measures

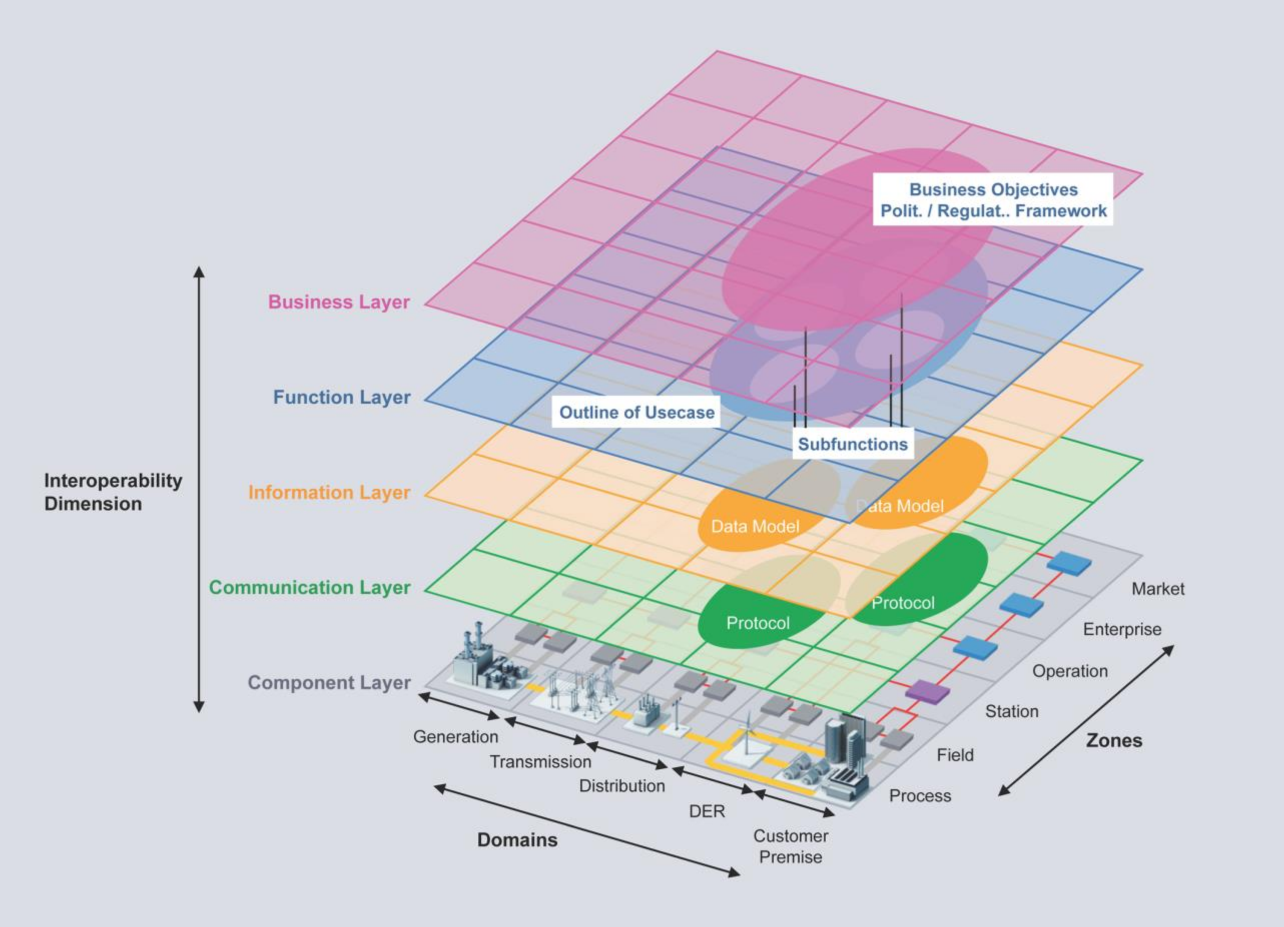
As mentioned in Section 3.1.1.1, availability and uptime of the power distribution systems are crucial. DR can assist in ensuring greater availability, but it relies on its enabling infrastructural technology, i.e. the smart grid. The smart grid stands to be optimised in the future thanks to better coordination of the various components involved in the processes through ICT communication (*Guidelines for Smart Grid Cybersecurity*, 2014).

To ensure that technical and non-technical requirements can be properly analysed, standardised technical models should be taken into account at design time (Suhr et al., 2013). Without standardised data models and interfaces, due to the large number of components involved, the overall costs for integrating new application would increase (Uslar et al., 2005).

In this context, the Smart Grid Architecture Model (SGAM) framework (*Smart Grid Reference Architecture*, 2012) is a recognized tool for analysis and mapping of smart grid use cases. The framework represents the Smart Grid and its use cases in five layers, each of them described as a bidimensional plane in which the first dimension represents the domains of the electrical energy conversion chain (i.e., Bulk Generation, Transmission, Distribution, DER, and Customer Premises), while the second one represents the hierarchical levels – or "zones" – of power system management (i.e., process, field, station, operation, enterprise, and market).

The five interoperable layers – component, communication, information, function, and business – considered in the SGAM framework allow to represent business and technical analysis regardless of the architectural and technological features of the smart grid.

Figure 3 - The Smart Grid Architecture Model

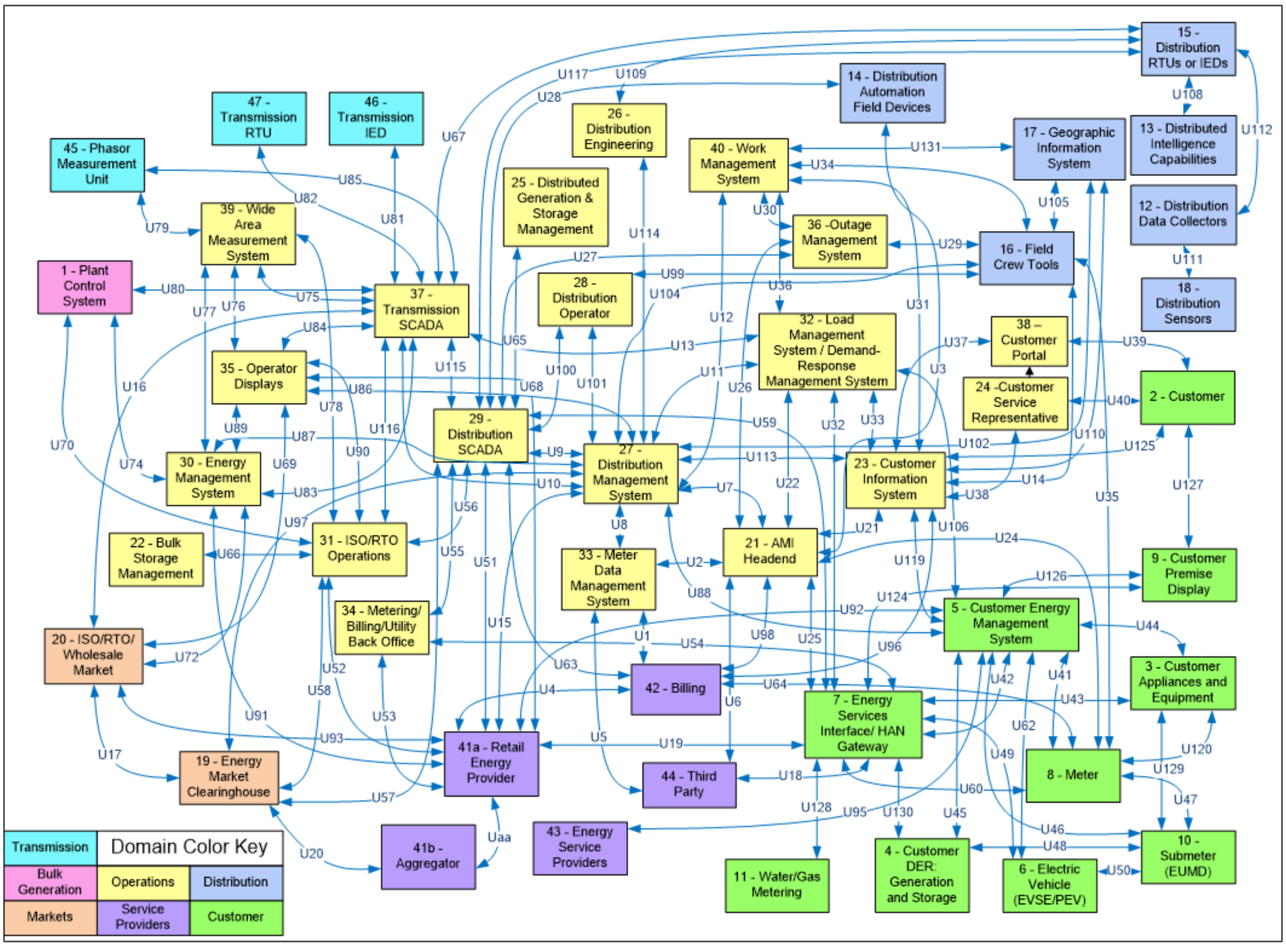


The model is depicted in Figure 3, where:

- The *Business Layer* focuses on strategic goals and processes while considering regulatory aspects;
- The *Function Layer* describes general use cases, functions, and services;
- The *Information Layer* describes the data models, enabling interoperability;
- The *Communication Layer* describes protocols and procedures used for data exchange;
- The *Component Layer* visualizes physical infrastructure and components.

As a critical infrastructure, security is crucial for the operation of the smart grid as a whole. For this reason, many standards exists with regards to it. One of them is the NISTIR 7628 (*Guidelines for Smart Grid Cybersecurity*, 2014), which is designed for end-to-end security. As Figure 4 shows, it includes a reference model composed of 46 actors distributed across 7 domain.

Figure 4 - NISTIR 7628 Reference Model


15 - Distribution RTUs or IEDs
14 - Distribution Automation Field Devices
47 - Transmission RTU
46 - Transmission IED
26 - Distribution Engineering
45 - Phasor Measurement Unit
40 - Work Management System
17 - Geographic Information System
13 - Distributed Intelligence Capabilities
25 - Distributed Generation & Storage Management
39 - Wide Area Measurement System
36 -Outage Management System
12 - Distribution Data Collectors
16 - Field Crew Tools
1 - Plant Control System
37 - Transmission SCADA
28 - Distribution Operator
18 - Distribution Sensors
32 - Load Management System / Demand-Response Management System
38 – Customer Portal
35 - Operator Displays
24 -Customer Service Representative
2 - Customer
29 - Distribution SCADA
27 - Distribution Management System
23 - Customer Information System
30 - Energy Management System
22 - Bulk Storage Management
31 - ISO/RTO Operations
21 - AMI Headend
33 - Meter Data Management System
9 - Customer Premise Display
34 - Metering/ Billing/Utility Back Office
5 - Customer Energy Management System
20 - ISO/RTO/ Wholesale Market
42 - Billing
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
41a - Retail Energy Provider
19 - Energy Market Clearinghouse
44 - Third Party
8 - Meter
41b - Aggregator
43 - Energy Service Providers
11 - Water/Gas Metering
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/PEV)
10 - Submeter (EUMD)
Transmission
Domain Color Key
Bulk Generation
Operations
Distribution
Markets
Service Providers
Customer
U117
U109
U28
U67
U85
U82
U81
U79
U114
U27
U80
U75
U77
U76
U84
U99
U104
U65
U115
U100
U101
U68
U16
U86
U78
U89
U87
U116
U90
U70
U74
U69
U83
U9
U10
U97
U56
U66
U55
U51
U8
U131
U34
U108
U112
U30
U105
U29
U36
U111
U12
U31
U13
U37
U3
U39
U11
U26
U40
U59
U32
U33
U102
U110
U125
U113
U7
U22
U14
U38
U35
U127
U21
U106
U24
U2
U119
U126
U72
U52
U58
U15
U1
U63
U4
U91
U53
U93
U5
U17
U57
U20
Uaa
U19
U88
U124
U92
U98
U25
U54
U96
U44
U42
U41
U64
U6
U43
U62
U49
U120
U129
U18
U60
U47
U128
U95
U130
U45
U46
U48
U50

The model identifies a list of 22 Logical Interfaces (LI) and, for each of them, describes the security requirements. The standard also describes privacy issues related to the technologies and information associated with the smart grid.

In an effort to combine the reference models used in Europe and the US with an eye towards improving the possibility of analysing the SGAM model from the security point of view, there are proposals from researchers to link NISTIR 7628 and SGAM (Uslar et al., 2014).

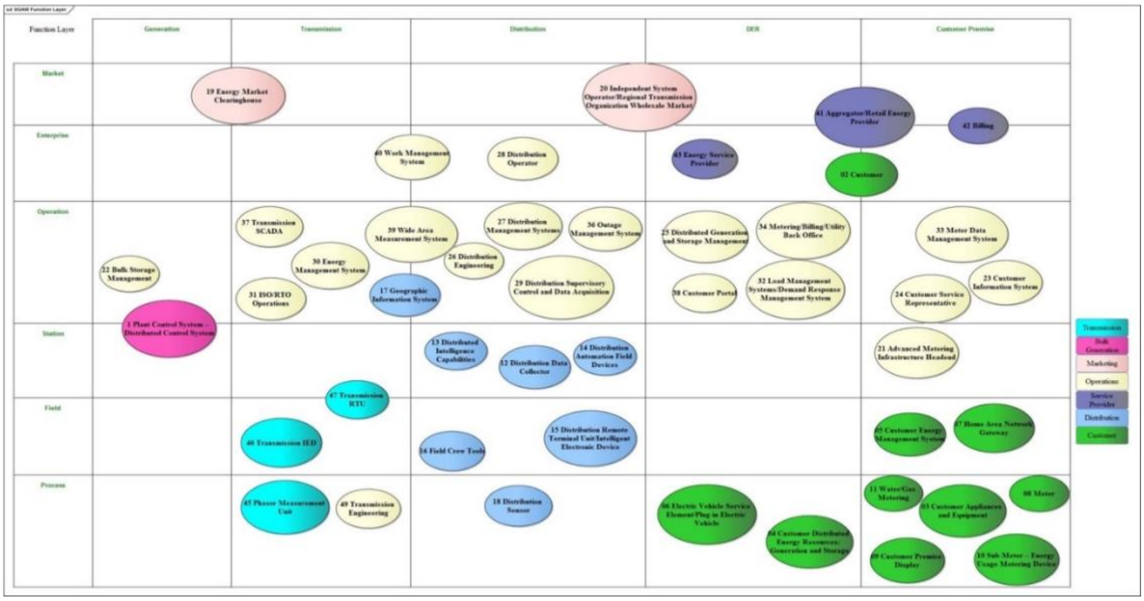
The mapping between NISTIR 7628 LI to SGAM planes can be done following a suggested list of steps. Once the two models are cross-referenced, the Smart Grid Cyber Security Requirements (SG-CySecReq) can be applied to SGAM. The list of suggested steps is reported below in Table 5.

Table 5 - Mapping LI to SGAM

Step #	Action	Description
1	Identifying and specifying the use cases	Use cases are identified, following standard actors and system lists.
2	Identification and mapping of Logical interfaces, com- munication links, and interface categories	System and interfaces are mapped to LI.
3	Integration of the LI onto the SGAM Functional layer	LI are integrated into SGAM on the functional layer. It is possible to stop here for a simpler analysis.
4	Assign the SG-CySecReq from NISTIR 7628	Protection goals and security standards for the use case are assessed using the SG-CySecReq.
5	Mapping to additional SGAM layers	Repeat the process for any additional SGAM plane required.

The complete mapping of the 46 LI to the SGAM functional layer is reported below, in Figure 5, where the original colors for of the NISTIR 7628 reference model are used.

Figure 5 - Complete mapping of NISTIR 7628 LI to the SGAM functional layer


sd SGAM Function Layer
Function Layer
Generation
Transmission
Distribution
DER
Customer Premise
Market
Enterprise
Operation
Station
Field
Process
19 Energy Market Clearinghouse
20 Independent System Operator/Regional Transmission Organization Wholesale Market
41 Aggregator/Retail Energy Provider
42 Billing
40 Work Management System
28 Distribution Operator
43 Energy Service Provider
02 Customer
37 Transmission SCADA
39 Wide Area Measurement System
27 Distribution Management Systems
36 Outage Management System
25 Distributed Generation and Storage Management
34 Metering/Billing/Utility Back Office
33 Meter Data Management System
22 Bulk Storage Management
30 Energy Management System
26 Distribution Engineering
29 Distribution Supervisory Control and Data Acquisition
38 Customer Portal
32 Load Management Systems/Demand Response Management System
24 Customer Service Representative
23 Customer Information System
31 ISO/RTO Operations
17 Geographic Information System
1 Plant Control System – Distributed Control System
13 Distributed Intelligence Capabilities
12 Distribution Data Collector
14 Distribution Automation Field Devices
21 Advanced Metering Infrastructure Headend
47 Transmission RTU
46 Transmission IED
16 Field Crew Tools
15 Distribution Remote Terminal Unit/Intelligent Electronic Device
05 Customer Energy Management System
07 Home Area Network Gateway
45 Phasor Measurement Unit
49 Transmission Engineering
18 Distribution Sensor
06 Electric Vehicle Service Element/Plug in Electric Vehicle
04 Customer Distributed Energy Resources: Generation and Storage
11 Water/Gas Metering
03 Customer Appliances and Equipment
08 Meter
09 Customer Premise Display
10 Sub Meter – Energy Usage Metering Device
Transmission
Bulk Generation
Marketing
Operations
Service Provider
Distribution
Customer

3.1.3 Cybersecurity requirements

After analysing the abovementioned legal framework and considering the structure of a smart grid (Mrabet et al., 2018), it has been possible to identify the macro-requirement for cybersecurity, and to subsequently split it into subrequirements illustrated in Table 6 - Security subrequirements. **The macrorequirement is demonstrated compliance with NISD, Cybersecurity Act, and state-of-the-art technical measures.** The subrequirements are also drawn from work by the National Institute of Standards and Technology[8] (which, despite being a US-based governmental organization, can provide guidance in this matter).

[8] https://www.nist.gov/

Table 6 - Security subrequirements

#ID	Requirement	Description
SSR1	Implementation of security measures (in general)	The IT infrastructure shall implement adequate and appropriate security measures able to protect the data to be ingested in the infrastructure as well as its functionalities. In this respect, such measures shall include either physical or technological measures, and in any case shall be designed applying a risk-based approach, which shall consider all the components and their interactions.
SSR2	Notification system	This requirement entails that the infrastructure is able to (i) detect and to send a prompt warning notification/message in case of actual attacks or even potential to the most appropriate authority; (ii) send a notification message complete with all the necessary information to detect the threats and determine the countermeasures; and (iii) the same notification system shall also be designed and construed applying adequate and proportionate security measures.
SSR3	Confidentiality	The requirement of confidentiality aims at protecting both personal and non-personal information from un-authorized access and/or use.
SSR4	Availability	Means that the information circulating within the smart grid are timely and reliably accessible in case of need.
SSR5	Integrity	Means that the information stored or in any case circulating within the IT infrastructure cannot be modified (nor be tampered or lost), and therefore is reliable and trustable. A good practice might be the implementation of a blockchain solution.
SSR6	Accountability	Entails that the data and the operations made on certain data can be tracked and traced back to specific and pre-authorised individuals.

3.1.4 Cybersecurity requirements as multi-dimensional risk mitigation and avoidance factors

With Table 6 - Security subrequirements in mind, it is also possible to identify a series of potential threats or potential concerns in Table 7.

Table 7 - Potential concerns or threats impacting security requirements

#ID	Requirement	Threats or potential concern
SSR1	Implementation of security measures (in general)	• STHR1 - appropriate security measures either at organizational and at technical level have not been developed/have been wrongly implemented. In particular, there might be the risk to cover all the identified potential threats (i.e. defined in D1.1) but the implementations are not sufficiently flexible to cover also unforeseen events; • STHR2 - an alignment among the security measures *strictu sensu* and the security measures implemented to ensure the privacy and data protection rights has not been performed and such dis-homogeneity might create conflicts.
SSR2	Notification system	STHR3 - the system has not been designed to provide timely alerts and/or the addressee of the alerts have not been correctly identified, or the alert chain is per se not secured and possible intrusions or interferences might happens jeopardising the alert system itself and the messages contained.
SSR3	Confidentiality	STHR4 – an improper definition and management of authorisations to access and/or use data might entails: (i) several vulnerabilities and impact on the confidentiality of its managed information; (ii) the violation of several GDPR provisions.
SSR4	Availability	STHR5 – overload of security operations might potentially impact on timely access to important information, necessary for the proper operating conditions of the smart grid.

SSR5	Integrity	STHR6 – data, flowing from EdgeNetwork devices to BRIGHT architecture, may be compromised either due to processing or to malicious tampering.
SSR6	Accountability	STHR7 – if any specific data transformation is performed without having ensured the traceability of authorised permissions, or permissions are not assigned to trustable entities, then it could be difficult if not impossible to reconstruct a chain of events.

The following table (Table 8) intends to provide a clear and practical guide to BRIGHT IT Partners when it comes to apply all the above mentioned considerations in developing the BRIGHT IT architecture and its relevant components. To develop and implement an appropriate IT solution, it is necessary to implement all the above mentioned requirements, in order to avoid - or at least mitigate - the impacts from potential concerns or threats.

One final remark: the following practical guidelines can be refined as soon as a technological improvement take place. As a consequence, the following should be considered as a "living document" that can be updated if needed.

Table 8 - BRIGHT compliance rules and cybergovernance policies

Impacted requirement	Potential concerns or threats	Rules and policies
SSR1	• STHR1 • STHR2	• It is recommended that ICT processes in the BRIGHT project consider for each component the definition of security test procedures, acceptance thresholds and reports in order to evaluate the addressing of all the defined threats, as well as to identify new potential and unforeseen threats. • It is recommended to release the BRIGHT components with relative test reports, in order to provide evidence of security level.
SSR2	STHR3	• It is recommended to promptly notify the parties (i.e. data subject and data controller) about the status of any event occurred in the system and that can directly or indirectly impact on them. • Notification system has to adopt appropriate measures in order to guarantee the authenticity and integrity of alerts themselves.
SSR3	STHR4	• It is recommended to define, implement and test appropriate management of authorisations to access and/or use data. • It is recommended to continuously update the level of reputation of the entities involved to gather, collect, access and process data. Based on the updated information, authorisation to access and/or use data have to be accordingly revised.
SSR4	STHR5	It is recommended to identify the reasonable level of security with respect to the time constraints. Lightweight hashing algorithms and performing encryption mechanisms should be considered at the design phase of the communication protocols and mechanisms of the architecture.
SSR5	STHR6	It is recommended to adopt techniques of data integrity management such as hashing, EDCs, etc.
SSR6	STHR7	It is recommended to ensure traceability of permissions, authorisations, reputations, events, and any vital information needed for providing evidence of system accountability.

4 Ethics

The ethics requirements in the following two sections differ from those put forward in WP10 at the start of the project. The latter strongly relate to the management of the project; in other words, they are normative and describe what should and should not be done in the project. Conversely, the requirements made explicit herein address what could be done with the project's outputs, i.e. its research, technology, and business practices, and are thus positive recommendations – "positive" in a philosophical sense, that is to say that it assists in making something effective, therefore synonymous of "productive" and "constructive." The collection of these positive ethics requirements and the associated measurement techniques make up the ethics framework of the BRIGHT project. The goal of this framework is to highlight ethics aspects that otherwise risk being overshadowed by routine, efficiency-maximizing operations connected to electrical and heating grids.

To develop the BRIGHT ethics requirements, we elucidate the difference between different branches of ethics at a high level. The overview offers a shared language and reasoning useful to applying ethics in the energy sector, as we do in sections 4.2 through 4.6, by identifying relevant aspects and explaining their relevance to BRIGHT. The details of the assessment of these requirements, which will be conducted by M36 of the project through SAT, CEL's methodology, can be found in Section 4.7, which concludes this part of the deliverable by also presenting a summary of the BRIGHT ethics framework.

4.1 Applying ethics to BRIGHT

Ethics is not concerned with the feelings that anyone can perceive to be an attitude, obligation, or duty towards someone or something. Those feelings are *morality*. **Ethical theory, like scientific theory, provides us with a mode of reasoning, i.e. a framework, for analysing moral issues via models that are internally coherent and consistent as well as comprehensive and systematic.**

According to some scholars, the primary goal of a moral system is to produce desirable consequences or outcomes for its members (van de Poel et al., 2011) For these ethicists, the consequences (i.e. the ends achieved) of actions and policies provide the ultimate standard against which moral decisions must be evaluated. So if one must choose between two courses of action, the morally correct action will be the one that produces the most desirable outcome. These scholars are known as utilitarians and consequentialists, and they argue that, in a given society, the effect or consequences of an action on the greatest number of individuals, i.e. the majority, is paramount in moral deliberation. **The main rules of utilitarian thought are** (Tavani, 2015)**:**

- **Morality is tied to the production of happiness or pleasure;**
- **Morality can ultimately be decided by consequences of either actions or policies.**

However, not all ethical scholars share this view: deontological ethics rejects all consequentialist ethical theories (Brey, 2013; Tavani, 2015; van de Poel et al., 2011). Immanuel Kant (1724–1804), the forefather of this branch of ethics, which derives its name from the Greek word *deon*, meaning duty, argued that morality must be built not on the effects of human actions, but on the concept of duty or obligation that humans have to one another. As such, morality has little or nothing to do with the promotion of happiness or the achievement of desirable consequences. In fact, in some instances, performing our duties may even result in our unhappiness and may not necessarily lead to consequences considered desirable. "Unlike animals who may be motivated only by sensory pleasure, humans have the ability to reason and deliberate. […] But because we have a rational capacity, we are able to reflect upon situations and make moral choices in a way that other kinds of (nonrational) creatures cannot" (Tavani, 2015 p. 57). The golden rule of this mode is:

Act always on that maxim or principle (or rule) that ensures that all individuals will be treated as ends-in-themselves and never merely as a means to an end.

Where utilitarian or deonthological principles could possibly be coded into a decision maker, a third branch of ethics, virtue ethics, explains actions not based on their consequences or intention, but on the virtues of the agent, such as courage and dignity. The fundamental principles of virtue ethics were introduced in the writings of Plato and Aristotle nearly 2,500 years ago. Both asserted that virtues can be built over time, via experience-based knowledge and evidence-based feedback that regulates specific actions against virtuous norms (Brey, 2013). Summing up, virtue ethics focuses on criteria having to do with the development of individuals and their acquisition of good traits and habits. The main rule of modern virtue ethics can be said to be (Tavani, 2015 pp 64-65):

Instead of asking, "What should I do in such and such a situation?" a virtue ethicist asks, "What kind of person should I be?" Hence, the emphasis on being a moral person, and not simply on understanding what moral rules are and how they apply in certain situations.

The brief primer in the preceding paragraphs serves to establish a common language for establishing BRIGHT requirements that favour an ethical approach to DR applications. In other words, the ethics requirements defined in this section allow moral action to occur not only in the BRIGHT DR instances, but also more broadly in the energy sector.

"Energy ethics" should aim to judge how to integrate energy services with non-energy services such as comfort, health, and safety. The maximization of profit and energy savings cannot be the sole, absolute values of the ethicality of similar energy operations. Energy ethics should adopt the best conceptual argumentations for promoting a solutions-oriented approach to ethical analyses when attempting to promote strategic research actions regarding the social acceptability of smart energy services both by framing the value conflicts occurring in the energy sector and by providing validation schemes for fostering trustworthy and acceptable data-driven energy services.

Therefore, **the "energy ethics" in BRIGHT can be considered a case of "business ethics," which can be thought of as the "study of the ethical dimensions of productive organizations and commercial activities"** (Moriarty, 2021). Though the BRIGHT consortium is a temporary grouping of organizations that are quite diverse in terms of their size, goals, and type of core activities, appreciating a discourse related to business ethics is important to ensure that the BRIGHT project considers the constraints of the energy sector while keeping in mind the realities of consumers' value bases and financial situations. For example, if services comparable to BRIGHT's are more accessible from a financial standpoint, then it stands to reason that there is likelier to be a wider consumer adoption. This would be not beneficial for both those involved in the research and for its sponsor, i.e. the European Commission. In other words, business ethics can be said to intersect utilitarian, deonthological, and virtue approaches, in the sense that it asks: "What kind of operational processes should there be to favour desirable consequences such that they treat all individuals involved as ends-in-themselves and not as a means to an end?"

To help answer this complex question, BRIGHT has put forward ethics requirements that address technological, environmental, social, and governance concerns, i.e. the major areas of most business operations. The BRIGHT ethics framework matches requirements to modes of measurement that consist in a mix of questionnaires and experiments both in the field and in the lab.

To help orient measurements, BRIGHT will employ SAT in T3.3, the proprietary method of consortium partner CEL. As far as business ethics is concerned, SAT has been developed against the backdrop of increased attention to so-called ESG investment practices, i.e. criteria and standards that both investors and consumers focus on when deciding to purchase respectively securities and products or services from a given company (Chen, 2021).

As Section 4.3 will explain in greater detail, the SAT approach involves the measurement of certain areas of consumers' perception of technology in key areas termed "bubbles," which in BRIGHT relate to the User Experience (UX) and Value Impact (VI). As mentioned in D3.1, consumers are resistant to DR programmes unless they are provided with a consistenly engaging UX. Engagement can occur through feedback systems, which are a way to stimulate adjustments in the face of external shocks (Åström & Murray, 2021; Smil, 2018). Put differently, feedback signals to users to align their consumption patterns with grid availability and, therefore, help achieve the United Nation's seventh SDG, Affordable and Clean Energy, as measured especially by the ratio of primary energy to GDP.[9]

D3.1 also extensively touched upon other factors of resistance to DR, such as trustability and privacy issues, something that will also be addressed in Section 4.3; these concepts are addressed and assessed in the VI bubble, hence its relevance for BRIGHT. Details of the assessment are described in Section 4.3, while the framework as a whole is presented in Section 4.7.

4.2 Responsible Research and Innovation ethics requirements

These requirements address the deonthology of scientific research that has an impact on services of public interest. The reason these requirements have been advanced is to ensure that primary and secondary stakeholders' expectations of the project – which include the project's beneficiaries, sponsor, the media, sector actors, and policy makers –are clear.

Technical partners are currently developing the technologies that will be tested in BRIGHT pilots. However, at the time of writing this deliverable, it is still not completely clear what mix of technologies will be deployed in each pilot. **Since by project design different technology mixes will be deployed across pilots that are *in se* diverse,[10] the research community should consider replicability recommendations emerging from BRIGHT as empirical and not scientific.** This is deonthologically important to state: it would be against research ethics to proclaim widespread benefits on the basis of results that may not be replicable in other contexts or with slightly changed technological mixes. In other words, BRIGHT's results will be circumscribed to the contingencies of the project's pilots.

This is not a problem *per se*, nor should it affect the perception of validity of the project as a whole. What is important is that stakeholders comprehend that BRIGHT replicability recommendations should be considered as modular and adaptable to the specific needs of new contexts that differ from those of the project. In these different contexts, actors could require certain features which were not developed in BRIGHT or desire to not deploy other features that were developed. This underscores an adherence to agile project management philosophy as opposed to rigorously scientific experimentation.

However, if the project's ambition were to deliver replicability guidelines considered universally valid, conducting in lab experiments that isolate variables and that introduce greater controls would temper the relative lack of experimental rigour. Consumer feedback will provide insight into the relevance of this aspect in their perception of BRIGHT. Their perception will be assessed through questionnaire responses collected during the pilots.

To sum up, the responsible research and innovation ethics requirement of BRIGHT is:

[9] https://sdgs.un.org/goals/goal7

[10] Though it may seem obvious, it seems useful to remind the reader that pilots are diverse due to geographical, cultural, historical, and other types of variables that impact the pilot's participants and its locale.

ER1. The BRIGHT project should make a sufficient effort to represent replicability recommendations as empirical and not scientific

4.3 Ethics of technology requirements

Quite a young field, ethics of technology tries to forecast the possible ethical implications of technological innovations. To ensure that technologies are "ethical" means to verify their adherence to human values and human rights by going beyond purely legal aspects connected to the introduction of a technological innovation by, in many cases, framing issues that the legislation will then tackle. So, while law addresses the difference between what is just and what is unjust, the ethics of technology – being a practical discipline of ethics, the branch of philosophy that studies right and wrong actions – addresses the difference between a right and a wrong use of technology. Generally, ethics of technology concerns itself with two issues: the ethicality of a technology per se, for example human cloning, and the impact that a given technology might have on a given society, for example the impact of social networks (not ethically problematic per se) on human sociality. The first dimension concerns the design of a technology; the second dimension, its impact. In these two directions, often compenetrating each other, we outline the relevance of ethics of technology for the BRIGHT project.

As stated in the

Introduction, BRIGHT will involve the use of AI algorithms at large scale in order to maximize the effectiveness of DR. While Section 2 addressed issues relevant to privacy and data protection, ethics of technology addresses ethical concerns of accountability, fairness, and so forth, connected to the increased use of AI systems today.

In the European Union today, there are two main common pillars on which to base an assessment of compliance of technological innovations with ethics. These are "Ethics Guidelines for Trustworthy AI", the white paper by the High Level Expert Group (HLEG) on AI appointed by the EU commission (*Ethics Guidelines for Trustworthy AI*, 2019) and the brand-new proposal for the European Regulation on AI (*Proposal for a Regulation on a European Approach for Artificial Intelligence*, 2021).

The white paper, which is not binding but has become a milestone for the development and design of ethics approaches to AI, provides the 7 key requirements on which the evaluation of the ethicality of an AI-based technology should rely:

1) Human agency and oversight
2) Technical Robustness and safety
3) Privacy and data governance
4) Transparency
5) Diversity, non-discrimination and fairness
6) Societal and environmental well-being
7) Accountability (see also PR7 in Table 2 for the link between accountability and data protection)

The EU proposal for the regulation of AI, on the other hand, wants to put in practice these suggestions by taking a risk-based approach in order to regulate AI systems, which the Commission has divided them into three main groups. A small group of AI systems are banned and prohibited, for example AI algorithms that allow a government to give social credit scores to a population. Others are considered high-risk and need specific precautions: "For high-risk AI systems, the requirements of high quality data, documentation and traceability, transparency, human oversight, accuracy and robustness, are strictly necessary to mitigate the risks to fundamental rights and safety posed by AI and that are not covered by other existing legal frameworks." .

In general, for an AI system to be considered high-risk it should fulfill both of the following conditions (*Proposal for a Regulation on a European Approach for Artificial Intelligence*, 2021, p.8):

1) AI systems intended to be used in any of the areas listed in points 1 to 8 of Annex III[11];
2) AI systems that pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

Moreover, Annex III at point 2 states that any AI algorithm tasked with the "management and operation of critical infrastructure: AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity" should be considered as high risk. **Since BRIGHT involves energy infrastructures, based on the EU proposal for the regulation of AI, the implementation of AI will imply that the project deals with high-risk AI, if and only if AI systems are integrated into safety components. Otherwise, BRIGHT will not include high risk AI systems.**

Of the 7 principles outlined by the HLEG, BRIGHT will surely have to deal with the last four, since it will involve AI systems in DR: this may affect both individuals from an economic point of view and society as a whole in the way of managing the distribution of energy.

On the individual dimension, the fairness of the algorithm must be ensured in order to avoid unwanted and unforeseen discrimination of groups or individuals, affecting their access or ability to operate in the DR environment. On the collective dimension, it is necessary to prevent bias from polluting the AI dataset both to ensure fairness and to avoid unexpected shortcomings in the behavior of the DR system. In order to ensure this, the criteria which the AI algorithms will use in order to forecast the individual and the collective behavior should be accountable and explainable.

In addition to the compliance with the ethical frameworks envisioned by the EU commision, we will evaluate the BRIGHT technologies under a conceptual framework developed by CEL. This framework, which has been mentioned in Section 4.1, aims at evaluating the expected Social Acceptance of Technology (from which its acronym, SAT) in a given context/society. We claim that the compliance of a technology with the ethical requirements of the EU does not exhaust the discussion on the social impact and acceptability of a technology in a society. The social acceptability of a technology might be affected by psychological features, user experience, or by the impact that the given technology might have on the values of a given social context. All these issues should be carefully evaluated in order to guarantee that the technology will be welcomed by the individuals of a social context, and to avoid mistrust in institutions.

The SAT methodology, therefore, will have the duty to assess if the BRIGHT project is able to put in place socially acceptable technologies and to communicate their usage, benefits, and risks in a correct way. The research model of the method is structured around conceptual constructs – which we have called "bubbles" – that identify the four fundamental areas of evaluation on which the method is based. The model itself has the feature of being modular and scalable.

[11] Except for point 2, discussed below, the others are not relevant for BRIGHT.

- **"User-Experience Satisfaction"**: This first bubble aims to understand how the user interacts with the technological product, also considering the content conveyed by brand communication and marketing.
- **"Value Impact"**: This bubble evaluates the extent to which the technology concerned and – perhaps even more importantly – the company producing it, comply with shared social values. CEL researchers will consider not only cultural values, but also the specific values of each stakeholder community. Esempio: Privacy e Trust

In order to better understand the utility of the SAT methodology for the BRIGHT project we provide two examples of its application:

1) For what concerns the user experience bubble, it is important to assess what is the relation between the perceived usage of the user, the expectation that s/he has about the technology and the communication strategies put in place by the partners involved in the pilots.
   In fact, the user experience of a technology deeply impacts its adoption by users and the overall satisfaction of stakeholders. The usage or the benefits of a technological product might not be directly understood by users: this may bring users to opt-out from a DR program or to participate in an incorrect way, as we already highlighted in the deliverable 3.1. The assessment of the communication strategies, and their amendment and correction, is important for the BRIGHT's pilots in order to maximaze the participations and the engagement. The SAT methodology is able to assess if the three dimensions – the usage, the expectations and the communication – are coherent with the project's goals in terms of users engagement.
2) Regarding the value impact bubble, an example of SAT evaluation is the case of the perceived trustworthiness of a technology inside a community. Many elements impact this feature: the perceived compliance of the company producing it with the community values, it is impacting if the technology produces for example social exclusion etc. Surely, of great importance for the BRIGHT project is the impact on the DR trustworthiness of the privacy dimension. In fact, as pointed out in 3.1, part of the users are often concerned with the privacy issues of smart meters and are not likely to accept what might be perceived as a constant and intrusive monitoring. In SAT we will understand how the privacy issues may impact on the DR trustworthiness.

An important point to underline is that SAT does not evaluate the objectiveness of the parameters, for example the benefits that an object could bring in the users life. SAT remains on the perceptual level measuring what users and stakeholders think about the usefulness of the technological object. The same goes for the value-related evaluations: SAT is not concerned with judging the rightness of the values conveyed by a technology, instead it measures the users' perception of the value impact. Since the BRIGHT project, at the current stage, has not specified the technical functioning of the AI algorithm that it will implement in order to improve the DR system, we cannot give precise and detailed suggestions to ensure ethicality. Nevertheless, observing the following requirements will ensure the ethicality of the technologies adopted in BRIGHT:

ER2. BRIGHT puts in place the requirements set by the EU proposal on AI regulation

ER3. BRIGHT considers that, under the conditions specified in Annex III of the Commission's proposed regulations, its AI algorithms might be viewed as high-risk. This condition

depends on the use of AI systems: only if integrated in safety components it should be considered high-risk.

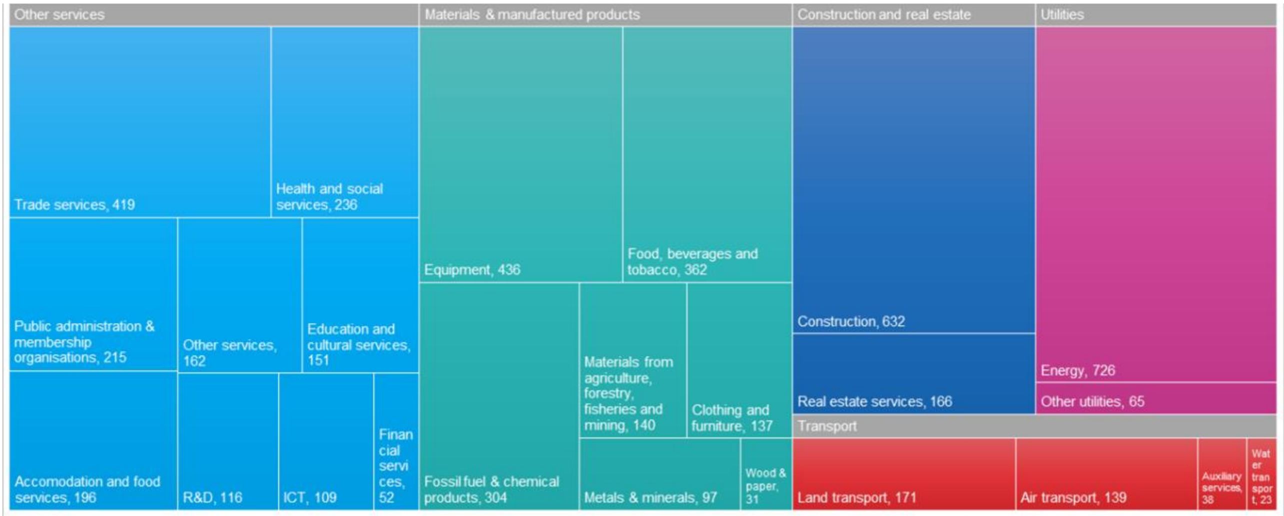
ER4. BRIGHT makes an effective effort to forecast the possible issues of fairness in the DR program

ER5. BRIGHT puts in place communication efforts towards the pilot participants that enhance the social acceptability of the technologies implemented. These communication strategies will include, but not be limited to, online and physical means and should aim to correctly communicate the ways to use the technologies implemented in the pilots, in order to avoid false expectations

4.4 Environmental ethics requirements

In light of climate change and to reduce related risks such as €190 billion in annual losses for a 3°C rise in temperatures (Ciscar et al., 2014), the European Union has launched an ambitious set of policy packages, also known as the Green Deal, to make its economy carbon neutral by 2050 (*A European Green Deal: Striving to Be the First Climate-Neutral Continent*, 2019). Figure 6 shows that energy products (top right corner in fuscia) – as classified by EUROSTAT's 2008 Classification of Products by Activity (CPA) – have the largest footprint in CO_2 kilos per person.

Figure 6 - CO2 footprints by product group, EU27, 2019



Source: Eurostat env_ac_io10 *https://ec.europa.eu/eurostat/databrowser/view/env_ac_io10/default/table?lang=en*

Therefore, the energy sector is under both a strong policy push and moral obligation to green its output. Fortunately, solutions exist, and these include DR, which has solid indirect environmental benefits on an economy.

One environmental benefit of DR is that it would help align supply and demand, moving generation away from forecasting models to near-real time signals. For example, in the case of the Italian pilot, owners of electric vehicles will be incentivized to use their vehicles to supply flexibility to ASM as the DSO. Thanks to the incentives, vehicle owners should recharge their batteries at times of day in which there is an excess of energy in the grid. In this scenario, the amount of energy necessary for EVs charging sessions is supplied by renewable distributed generation. Therefore, a reduction of CO_2 emissions from conventional production plants is achieved in an amount approximately equal to 300 gr. of CO2 per kWh (which, according to ISPRA, Italian Institute for Environmental Protection, is the average quantity of CO_2 per kWh purchased on the wholesale energy market by retailers) (*Fattori Di Emissione Atmosferica Di Gas a Effetto Serra Nel Settore Elettrico Nazionale e Nei Principali Paesi Europei*, 2020). Given that the quantity of energy supplied to the vehicles during the

Italian pilot will be measurable, it will be possible to also measure savings in terms of CO_2 emissions by the end of the project.

However, BRIGHT is more complex than the study of which consumer incentives are more likely to favour DR. Indeed, the project aims to apply technologies such as AI to improve the DR performance. In WP4, researchers will develop time-series forecasting techniques, models, and control algorithms for flexibility and energy production and consumption values to predict energy at fine-grain scales (customers, communities, etc.) using Big Data, digital twins, and ML. Training such ML models tends to be resource-intensive from an electricity perspective, such that the amount of resources used is proportional to the number of actors at the scale for which the models are trained. With the focus on using deep neural networks necessary for these tasks, the energy footprint related to this research can be associated with two main categories:

i. training of these models
ii. searching for hyper-parameters that optimize the performance of these models.

For the first part, the plan is to measure the energy required for training by comparing it with the total time required for training a single model. With this metric, it will be possible to estimate the energy consumed as well as other impact points like CO2 consumed. Conventionally, these forecasting techniques require a large amount of data and are also inefficient in generalizing between different scenarios. Consequently, individual models need to be trained specifically for each entity/prosumer, significantly increasing the training times and hence the energy requirements as well. To offset this, BRIGHT technical partners are focusing on developing models using a novel neural network architecture, commonly referred to as Physics Informed Neural Networks. These networks use the physics of the system as input, which will lead to, among other things, lesser training data needed and hence reduction in training time. Furthermore, BRIGHT technical partners also plan to leverage the results from the Clustering and Segmentation task (T4.4) to identify entities/prosumers with similar behavior and build models for these clusters instead of individuals. This procedure has the potential of decreasing the number of models from a few hundred to less than ten (i.e., the number of clusters), and thus to reduce the overall energy footprint by reducing the number of trainings.

The second part involves hyperparameter search and tuning, which is a key part of any ML model and often requires many computations. BRIGHT technical partners are currently working towards identifying a suitable metric to measure the energy consumption over this search operation, after which we will investigate techniques to speed up this search. The plan is to conduct similar analyses for tasks in WP5, where the focus would be on using reinforcement learning algorithms to obtain optimum control policies.

Lastly, it's important to calculate not only the start-up environmental costs, but also operational ones. BRIGHT partners in WP4 will offer a provisional cost model for assessing such a footprint in the replication recommendations. It is important to note, at this stage, that said activity is non-trivial and dependent on various contextual variables. The goal, however, is to create ML algorithms that are energy-aware by design.

To sum up: the case of the Italian pilot and the gravity of the global climate situation suggest the following environmental ethics requirements:

ER6. BRIGHT should show whether the technologies used in the project contribute to reducing negative environmental impacts

ER7. BRIGHT should assess whether the environmental dimension is relevant in motivating consumers' choices to adopt DR solutions

4.5 Governance ethics requirements

Before addressing the "S" in ESG, we will focus on the "G" for reasons that will become apparent shortly. Generally speaking, governance is the set of processes an organization has in place for the management of its activities. For instance, in the public sector, government agencies' leadership is appointed by publicly elected (or otherwise appointed) officials to manage public goods or services, such as city parks or civil courts. Conversely, in the private sector, most large companies – especially if traded on a stock exchange – have a Board of Directors elected by shareholders; the Board, in turn, appoints a group of executives to conduct the company's undertaking, that is managing the production and distribution of a private good or service such as bread or, more relevantly for BRIGHT, meter-to-cash monitoring.

The finality of the two sectors is quite different: while public organizations aim to ensure that what they manage remains accessible to all at no or very low costs, private companies aim – with an exception being made for not-for-profit entities – to maximise the profitability of their undertaking. Nevertheless, in either sector, the quality of governance seems to both impact and be impacted by the quality of the business outcome; in other words, one key aspect for guaranteeing a desired level of quality for a business is to ensure that effective governance processes are in place (de Villiers & Dimes, 2021).

It should now be clear that the BRIGHT ethics requirements take governance elements into account to ensure the highest overall quality of the project's results. Before delving into the governance elements, we provide a brief overview of relevant literature. The main assumption – which will be validated later in this section – is that governnace processes *in se* shape business outcomes more than the people appointed to manage those processes. In other words, we assume that procedural aspects of governance affect outcomes organizations yield in social contexts.

Today, analysing and measuring the quality of governance in both the private and public sectors is the subject of much debate (Francesco & Guaschino, 2020). Despite many divergences in opinion, what most scholars agree upon is that the aforementioned distinction between two types of goods, i.e. private and public, is too simplistic. A richer categorization is needed. One of the most widely accepted classifications of goods is the one provided by politcal economist Elinor Ostrom (Ostrom, 2005) and shown in Table 9.

Table 9 - Four types of goods

		Subtractability of use	
		High	**Low**
Excludability from use	**Difficult**	*Common-pool resources*	*Public goods*
	Easy	*Private goods*	*Toll goods*

As can be seen, the type of good varies according to

a) how difficult it is to exclude beneficiaries from their use and
b) how much each use of a good diminishes another party's ability to use the same good later.

For the sake of clarity, some examples of each type of goods are as follows:

- **Common-pool resource** – a fishery: regardless of its size, it is more difficult to exclude someone from benefitting from a fishery; however, each time they do, they diminish the quantity of resource (e.g. fish) available to the next beneficiary.
- **Public good** – a sunset: it would be quite difficult to impede someone from admiring a beautiful sunset in a given location; furthermore, their admiration of the scene does not diminish the admiration someone else might be experiencing at the same moment.
- **Private good** – a plot of land: it is easy to lock off portions of land (e.g. by building an enclosure); each time exclusion of land from others occurs, there is less land for everyone else to benefit from individually.
- **Toll good** – a membership in a club: it is easy to exclude the next person from membership (e.g. through an entry fee), but if they join, they do not hinder previous members from using their membership.

The BRIGHT project deals with one specific good, chiefly local energy communities' flexibility trading systems (Hall et al., 2019), for which the above categorization is of particular importance. In fact, at the local level, excluding a participant from the trading system could be as difficult as excluding a beneficiary from a fishery. Similarly, one individual could overconsume flexibility just as another could overconsume fish; both cases would result in the depletion of the overall amount of resource available for future use by others.

But what could spur the overconsumption of common-pool resources? In answering the question, Ostrom (Ostrom, 2005, p.104) adopted the hypothesis of **"bounded rationality"** (Simon, 1957), which contradicts the typical assumption of utterly rational, utility-maximizing individuals advanced by neoclassical economics (Mill, 1844). "Bounded rationality" hypothesizes the following:

a) human beings do not always have access to all the information necessary to make an optimal decision prior to making it;

b) consequently, human beings make decisions based on heuristics, i.e. mental shortcuts.

While rationally constrained, humans are capable of updating their decision-making heuristics in relation to the management of common-pool resources by learning from experience. The question, at this point, becomes: "What are the contextual variables that can favour individuals' propensity to ameliorate the way they manage common-pool resources?"

A further premise is necessary to answer this question. Indeed, **given that the management of common-pool resources tends to be a collective effort in which trust and cooperation are essential, it follows that said management must follow specific rules**. Thus, a new question can be added to the previous one: "What rules help build trust and cooperation in scenarios in which more or less defined net benefits are at stake?"

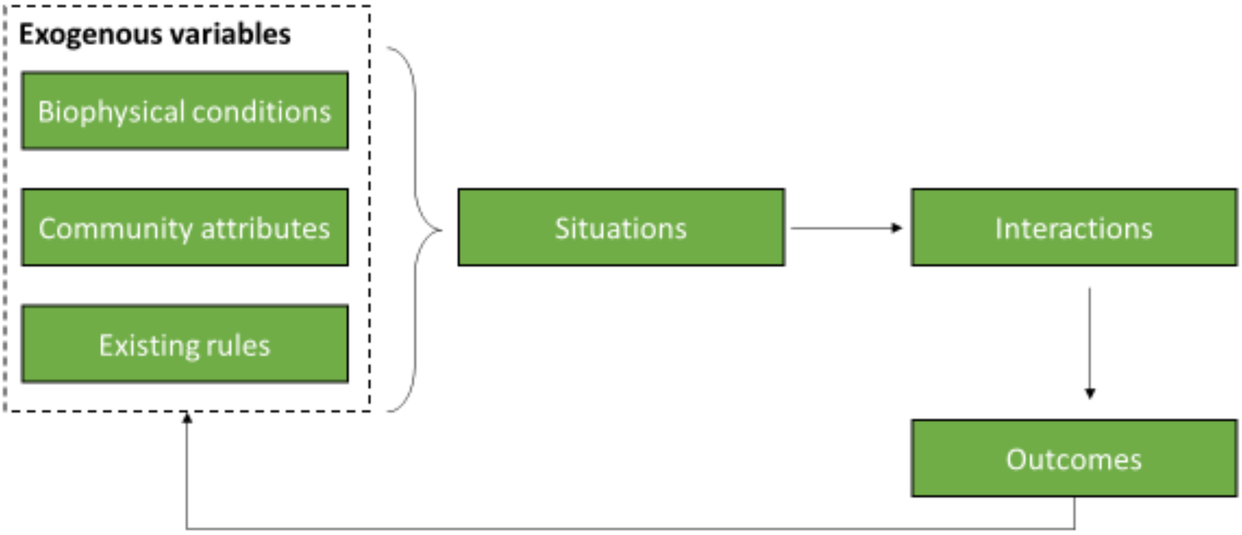
In order to be consistent with our positive ethics approach, we have not evaluated disincentive mechanisms such as punishment or fines for overharvesting. Instead, we rely on the work of Elinor Ostrom, who won the Nobel Prize in her field in 2009 for showing, through the development of an analytical framework based on field studies and laboratory experiments, how exogenous variables, rights, and rules shape the outcomes of interactions among individuals tasked in governing common-pool resources situations. Based on her work, we propose pragmatic ethical implications for a project such as BRIGHT and harken to a successful example of local energy management from recent history in the energy sector. The key: below a level of complexity that might require intervention by a central regulatory authority, local communities are able to self-manage a common-pool resource without overusing it by adopting a pertinent juridical form and governance model, such as those described in Section 5.2.1.3.

The following three exogenous variables influence any given situation in which a community debates the management of common-pool resources:

1. **Biophysical conditions**: the material factors that impact a community, such as the natural environment in which it exists, its geographical location, weather patterns, etc.
2. **Community attributes**: the history, the pre-existing knowledge, the degree of homogeneity, and the levels of human and social capital inherent to the community.
3. **Existing rules**: any pre-ordained norms that establish a common understanding of who must, must not, or may take action.

Figure 7 shows how exogenous variables influence situations, which in turn determine the interactions between members of a community. Together, they establish the final outcomes on the basis of the **property rights** they hold with respect to the common-pool resource in question.[12] Interactions, and their governing mechanisms, therefore, are the focal point of Ostrom's analysis, which will aid in establishing the specificities of interactions in BRIGHT.

Figure 7 - The relationship between exogenous variables, situation-based interactions, and outcomes in the governance of common-pool resources according to E. Ostrom



There are five property rights that individuals involved in an interaction may hold. These are:

1. **The right to access**: the right to physically or virtually approach a common-pool resource;
2. **The right to withdrawal**: the right to benefit from that resource;
3. **The right to manage**: the right to regulate internal the use patterns for that resource;
4. **The right to exclude**: the right to decide who who will not have the previous three rights;
5. **The right to alienate**: the right to sell or lease any of the previous four rights.

[12] Said property rights could foresee co-ownership structures, guaranteed through juridical forms such as cooperatives.

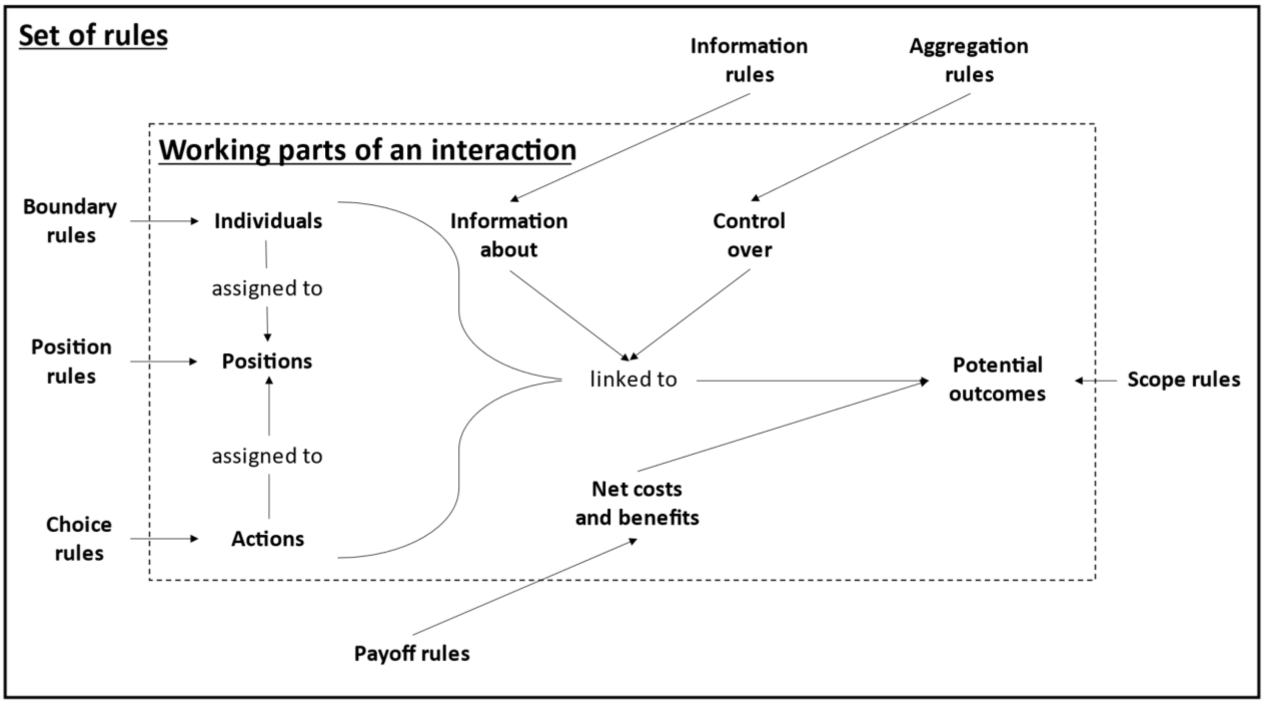
Every interaction over the management of a common-pool resource involves exercising one or more of these rights at a given point in time. Each exercise of rights occurs thanks to “working parts” governed by specific rules, summarized in Table 10.

Table 10 - The seven working parts of an interaction and their associated type of rule according to E. Ostrom

N.	Working parts of an interaction	Associated type of rule
1)	*Characteristics of the individuals* The degree of social, cultural, juridical, and economic heterogeneity, levels of knowledge, etc., of the individuals involved in the interaction	*Boundary rules* How are individuals chosen?
2)	*Positions the individuals hold* At any given point in time during the interaction, each individual in the interaction will occupy a certain role	*Position rules* What positions can be occupied? How many individuals can be in each position?
3)	*Actions that individuals can take at a specific point in time* Individuals may or may not make a certain decision / action at a point during the interaction	*Choice rules* What actions can individuals make?
4)	*Amount of information available* Individuals can know only the information available at a given point in time	*Information rules* What channels of communication can be used? What information can and cannot be shared?
5)	*Outcomes affected by the individuals’ actions* The actions of individual in given positions influence the outcomes of the interactions	*Scope rules* What outcomes can be affected and how?
6)	*The amount of control individuals can exercise* In affecting outcomes, individuals exercise diverse levels of controls	*Aggregation rules* Do majority or unanimity criteria apply How are actions at specific point mapped to outcomes?
7)	*Benefits and costs assigned to the outcomes* Individuals assign benefits netted of costs to each outcome.	*Payoff rules* How are benefits and costs to be distributed?

For the sake of completeness, “individuals” can refer to not only persons, but also to corporations or other legal entities involved in interactions. Boundary, position, and choice rules regulate who, how, and what actions can be taken considering the influence individuals can over the course of the actions, a position, or an outcome. Per the bounded rationality hypothesis, each action taken considers only a limited amount of the information avaialble at the time for a position. Ostrom (Ostrom, 2005, pp.40-41) defines positions as “classes” or “anonymous slots” that connect individuals to action. For further clarity, Figure 8 shows how each of the elements relates to the other.

Figure 8 - The elements of an interaction system according to E. Ostrom



The theoretical background to Figure 8, developed by Ostrom, supports our assumption that **procedural aspects of governance affect the outcomes organizations of individuals yield in social contexts more than the individuals themselves do**. Indeed, individuals are only one of the many working parts of an interaction, which is bounded by different kinds of rules. Favourable rules aid individuals in:

- establishing their reputations to each other;
- exchanging relevant information;
- defining capacity to enter and to exit the interaction.

So, to answer the two questions posed previously, rules are variables that can favour the betterment of management of a common-pool resource in a scenario in which different classes of individuals stand to gain differently from the resource itself.

Figure 9 - The logo of the Magliano Alpi Energy Community

This high-level, institutionalist view of governance may seem too abstract compared to the concrete reality of BRIGHT. This is not true, as **the discussed framework is applicable to the cases of many energy communities, for instance that of Magliano Alpi** (a town of 2.166 people[13] about 70 kilometres south of Turin in the province of Cuneo in the Italian region Piemonte). The local administration installed a 20 kWp photovoltaic panel on a portion of the city hall building roof. Energy in excess will be shared through the grid to other local public administration buildings and to several households. The project, which has galvanized neighboring communities as well, was able to be completed because of the involvement and support of citizens,

[13] http://dati.istat.it/Index.aspx?QueryId=18540

constant information exchanges, and clear definition of rights, roles, and responsibilities (Patrucco, 2020).

In essence, the Magliano Alpi case exemplifies and matches Ostrom's criteria of a well-run interaction leading to mutually agreed upon beneficial outcomes, thus allowing to put forward the BRIGHT governance ethics requirements:

ER8. BRIGHT communicates to individuals participating in local energy communities their rights with respect to any resource that can be considered common-pool

ER9. BRIGHT defines all seven rules governing interactions as they apply to each of the pilots, with special focus on the pemissible information exchanges, choices, and payoffs

ER10. In each of the pilots, BRIGHT takes into account pilot participants' feedback in establishing outcomes that are mutually agreed

4.6 Social ethics requirements

As stated in the previous section, our main assumption – supported by Ostrom's theoritical background – is that there exists a strong causal relation between effectiveness of governance and social manifestations of business outcomes. For this reason, we have addressed social requirements last, despite them traditionally appearing second in ESG practices.

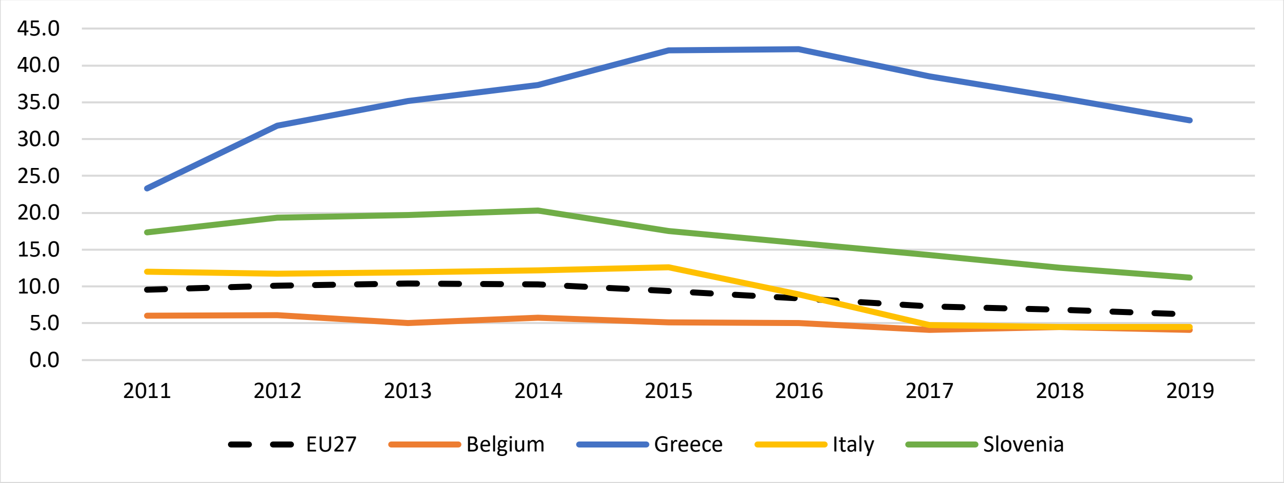
Out of all the business ethics requirements in BRIGHT, the social ones address the degree of inclusivity of business outcomes, i.e. the extent to which those who might be excluded for reasons including but not limited to their social, cultural, or economic status, can access benefits of the product or service offered..

On a broader scale, the inclusion of social ethics requirements is connected to the theme of energy poverty. Those vulnerable to energy poverty are often also vulnerable to other societal ills, such as poverty or discrimination (Großmann & Kahlheber, 2017).

Figure 10 graphs survey data gathered by EUROSTAT that shows how the share of households that default on utility bills is noticeably higher than the EU average in two of the four selected countries for the data range available, and far too high in comparison to SDG 7's Target 1, i.e. universal access to electricity by 2030[14]. However, DR solutions can contribute to a reduction of costs and, thus, to an achievement of the SDG's target. For instance, in Greece the average annual gas cost is between €700 and €1.000 for a typical household. Considering the average energy efficiency improvement of 15% - 35% for the domX heating controller solution, the initial investment cost of €150 (€120€ for the hardware and €30 for the installation) can be immediately covered over the first heating season in most cases.

[14] https://sdgs.un.org/goals/goal7

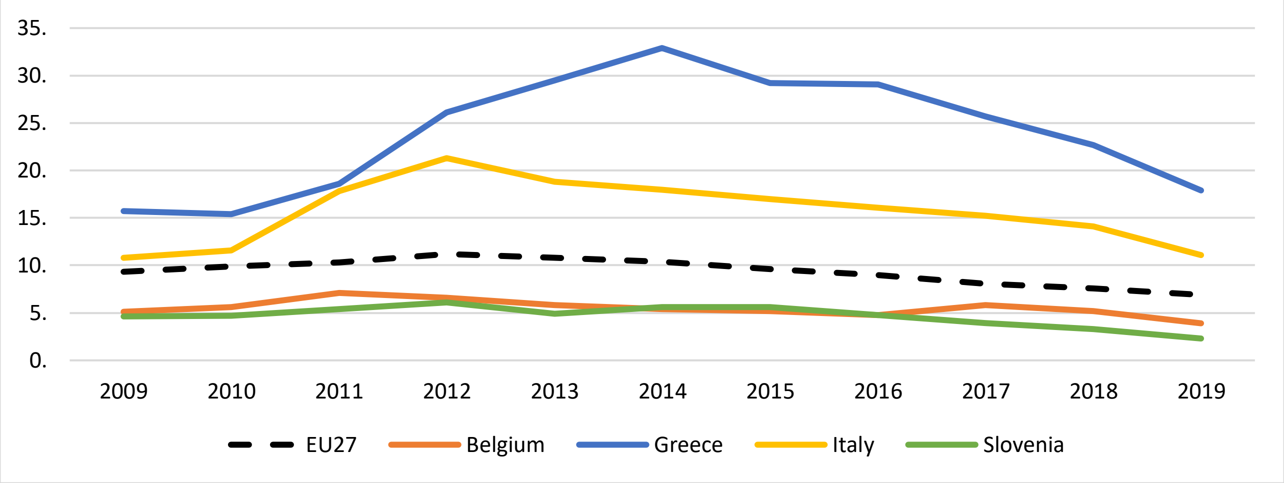
Figure 10 - % of households unable to pay utility bills on time in the past 12 months in BRIGHT pilot countries compared to EU27 average, 2011 - 2019



Source: Eurostat ilc_mdes07 https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=ilc_mdes07

In addition, Figure 11 shows that the share of the total population in the same countries that is unable to adequately warm their homes, is consistently higher than the EU average in again two out of four selected countries over a ten-year period.

Figure 11 - % of population unable to keep home adequately warm in BRIGHT pilot countries compared to EU27 average, 2009 - 2019



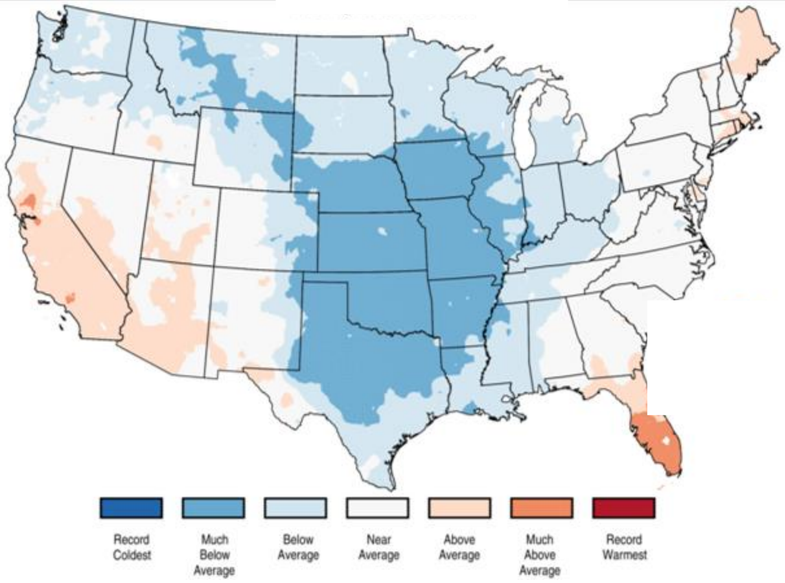
Source: Eurostat SDG_07_60 https://ec.europa.eu/eurostat/databrowser/product/view/ILC_MDES01

Both figures illustrate manifestations of "energy poverty", i.e. the condition of lacking "adequate energy services in the home" (*EU Energy Poverty Observatory*, 2021). **Actors in the energy sector are invited to reflect on underlying causes of and potential solutions to this social phenomenon.** Indeed, if market and regulatory factors do not shift in such a way to favour the achievement of SDG 7 goals, then certain risks are more likely to impact European society. A case in point is the mismanagement of the February 2021 energy crisis in Texas and other parts of the United States.

Temperatures throughout the Central United States dropped to record lows due to unforeseen weather events. While similar events have grown in intensity over the years, their impact was not considered in this case. Figure 12, from the National Centers for Environmental Information, shows large portions of Texas and other areas in the central part of the continental United States in darker shades of blue: these areas were significantly colder in February 2021 than their long-term average (*Assessing the U.S. Climate in February 2021*, 2021).

The extreme and unusual temperatures caused a spike in demand for electricity and heat (*Extreme Cold & Winter Update #1*, 2021); however, due to strained infrastructure, supply could not keep up (Searcey, 2021). To manage constrained supply, distributors adopted two solutions: rolling blackouts and price spikes (Kelly et al., 2021). This caused many households to be exposed to the extreme cold and to resort to unorthodox heating methods. Consequently, frailer citizens falling victim to hypothermia and others inhaling excessive amounts of carbon monoxide created by the burning of unorthodox heat sources brought the death toll to more than 100 (Weber & Stengle, 2021).

Figure 12 - Mean February-2021 temperatures in the United States compared to the average of the period from 1895 to 2021



For BRIGHT, the lesson from this tragedy is to put forward proposals for solutions that can ensure the resilience of local communities to climate abnormalities. Solutions can relate to technical or economic means that favour that resilience, such as increasing a local grid's flexibility by interconnecting it to other neighboring grids or imposing a price ceiling upon the occurrence of similar scenarios. As evidenced by a report by economists from The Brattle Group (Weiss et al., 2018), DR for natural gas aimed at residential, commercial, and industrial clients could help shave demand peaks, especially in colder periods. This would reduce – in the short term – both reliance on less environmentally friendly fuels and price spikes for consumers. In the long term, DR for natural gas would help avoid operation and maintenance expenses on existing infrastructure or the cost of new infrastructure.

In Europe, one policy that has attempted to tackle energy poverty at a national level has been the so-called ***Bono Social de Electricidad* (BSE) in Spain**, that is a regionally-financed discount on the price of electricity for qualified households.[15] The outcomes and results of the policy are somewhat controversial. As of 2010, García Alvarez and Tol found that the BSE had no positive effect on energy poverty, which in the period examined had actually worsened (García Alvarez & Tol, 2020). However, in 2018, Rademaekers et. al found that the share of households under social tariffs had decreased since 2010 (Rademakers et al., 2018 p.159).

[15] https://www.bonosocial.gob.es/

The BSE specifies that an individual or a family is at risk of energy poverty if their annual income is below €11.279,38, that is 1,5 times the IRPEM, a government-established poverty line. There are also two technical requirements for qualifying for the discount, that is:

- having underwritten a utility contract with the Voluntary Price for the Small Consumer (VPSC) tariff system, which calculates the price of electricity on a daily and hourly basis in accordance with variations in energy market prices;
- the contracted supply must not exceed 10kW.

Consumers that meet the requirements above are categorized as "**vulnerable**" and receive a 25% discount on their bills. The BSE foresees the following other two categories for consumers who meet the same technical requirements, but who meet specified socioeconomic criteria (*European Social Policy Network Report*, 2018)

- **Severely vulnerable**: customers whose annual income is below 50% of the IRPEM;
- **Severely vulnerable at risk of social exclusion**: customers whose annual income is below 50% of the IRPEM and already receive financial assistance from the local and/or national government.

The European Social Policy Network has pinpointed the lack of costs for the Spanish federal government as a pro of the BSE, while it highlights regulatory overlap problems as an area for improvement (*European Social Policy Network Report*, 2018).
The overview of the energy poverty situation in BRIGHT's four pilot countries and of the risks and benefits of both the Texan tragedy and the BSE allow us to present the social ethics requirements for the project.

ER11. BRIGHT technical partners assess whether DR solutions tested in the project could increase resilience to extreme weather events

ER12. BRIGHT consortium partners in charge of pilots offer low-cost IoT solutions, which can offer high cost-effectiveness, considering that the initial investment cost can be covered during the first year of application

ER13. BRIGHT consortium partners in charge of pilots might include individuals vulnerable to energy poverty in their samples in order to assesse whether these consumers perceive the project's technology mixes as useful to reducing energy poverty

4.7 The ethics framework as a whole

The following synoptic table collects the elements listed in the previous sections, provides an explanation as to how each will be measured, and explains what risks each will help avoided or mitigate.

Table 11 - The BRIGHT ethics framework

ID#	Requirement	Ethics category	Measurement technique	Risk(s) avoided / mitigated
ER1.	The BRIGHT project should make a sufficient effort to represent replicability recommendations as empirical and not scientific.	Responsible Research and Innovation	Internal evaluation	Proclaiming widespread benefits on the basis of results

				that may not be replicable
ER2.	BRIGHT puts in place the requirements set by the EU proposal on AI regulation	Technologies	Internal evaluation	Not to be compliant with EU regulation
ER3.	BRIGHT considers that under the conditions specified in Annex III of the Commission’s proposed regulations, its AI algorithm might be viewed as high-risk	Technologies	Internal evaluation	To fall inside the high-risk AI category withouth addressing these risks
ER4.	BRIGHT makes an effective effort to forecast the possibile issues of fairness in the DR program and in the blockchain technology	Technologies	Questionnaires to project partners	Unforcasted discriminatory or unfair behavior due to polluted dataset of AI algorithm
ER5.	BRIGHT puts in place communication efforts towards the pilot participants that enhance the social acceptability of the technologies implemented. These communication strategies will include, but not limited to, online and physical means and should aim to correctly communicate the ways to use the technologies implemented in the pilots, in order to avoid false expectations.	Technologies	Questionnaires to pilot participants, field / lab experiments	Mismatch of expectations with actual usage.
ER6.	BRIGHT should show whether the technologies used in the project contribute to reducing negative environmental impacts.	Environmental	Internal evaluation	Negative perception; lack of usefulness in obtaining SDG 7 goals.
ER7.	BRIGHT should assess whether the environmental dimension is relevant in motivating consumers’ choices to adopt DR solutions.	Environmental	Questionnaire, Field / in lab experiments	Lack of technology acceptance
ER8.	BRIGHT communicates to individuals participating in local energy communities their rights with respect to any resource that can be considered common-pool.	Governance	Internal evaluation	Mismanagement of energy resources
ER9.	BRIGHT defines all seven rules governing interactions as they apply to each of the pilots, with special focus on the pemissible information exchanges, choices, and payoffs.	Governance	Questionnaires	Mismanagement of energy resources
ER10.	In each of the pilots, BRIGHT takes into account pilot participants’ feedback in establishing outcomes that are mutually agreed upon.	Governance	Questionnaires, in lab experiments	Mismanagement of energy resources
ER11.	BRIGHT technical partners assess whether DR solutions tested in the project could increase resilience to extreme weather events.	Social	Internal evaluation	Negative perception; lack of usefulness in obtaining SDG 7 goals.
ER12.	BRIGHT consortium partners in charge of pilots offer low-cost IoT solutions, which can offer high cost-effectiveness, considering that the initial investment cost can be covered during the first year of application	Social	Internal evaluation (calculate the actual energy costs and savings per consumer to derive the payback time for the initial investment)	Inability to pay utility bills.

ER13.	BRIGHT consortium partners in charge of pilots might include individuals vulnerable to energy poverty in their samples in order to assesses whether these consumers perceive the project's technology mixes as useful to reducing energy poverty.	Social	Questionnaires, field / lab experiments	Negative perception; lack of usefulness in obtaining SDG 7 goals.

5 Analyses of standards and sector-specific legislative packages for the extrapolation of requirements

Prior to overviewing the implications of the Clean Energy Package for energy DR technologies, we provide a preliminary list of technical standards applicable to devices used in DR.

5.1 Standards framework

In the BRIGHT project, extended use of specialised electrical equipment or devices is expected in lab-based experimentation, large-scale pilot-based demonstrations, and possible other horizontal activities, all of which will occur in WP7. It is likely that most of such electrical equipment will be already available on the market, although we expect that certain specialised functions will be newly designed, reused, refitted for the following purposes, which are not an exhaustive list:

- Measurement of electrical energy
- Communication (e.g., between devices and higher layer system software)
- Control and interaction between user and other devices

The exact purpose and use of such devices are going to be determined later in the project, especially during pilot demonstrations. In any case, electrical equipment and devices used must meet certain criteria regarding safety, measurement accuracy, electromagnetic interference, environment protection, etc. Even if use will be limited to controlled laboratory environments or demonstration sites, any electrical equipment or device that finds its way to the EU market must follow conformity assessment procedures for which its manufacturers are responsible.

It is not in scope of this section of this deliverable to completely describe said procedures or to provide complete guidelines for manufactures. What this section will provide is a summary of harmonised standards used in electric and electronic engineering.

A harmonised standard is a European standard developed by a recognised European Standards Organisation (CEN, CENELEC, or ETSI). It is created following a request from the European Commission to one of these organisations. Manufacturers, other economic operators, or conformity assessment bodies can use harmonised standards to demonstrate that products, services, or processes comply with relevant EU legislation.

EU policies affecting electrical and electronic engineering industries (EEI) cover 3 major areas:

- Electromagnetic compatibility (EMC)
- Low Voltage
- Radio Equipment

A special topic related to the scope of demand response (DR) regards measuring instruments.

All equipment must comply with Restriction of the use of certain hazardous substances (RoHS) for environmental safety purposes.

Additional need, for standards and normatives (in terms of proposals, amendments or even creation of new) may emerge during all activities within the project BRIGHT, esp. in areas protocol stacks. Such additional standardization activities will be carried out in Task 8.5 of Work Package 8.

5.1.1 Measuring instruments directive (MID)

With the entry into force of the Measuring Instruments Directive (MID, Directive 2014/32/EU)[16], the European Commission aimed to harmonise throughout Member States key aspects of measuring instruments ranging from water meters to weighing machines. These instruments are important for trade, consumers, and industry, as they ensure accuracy of measurement, transparency and fairness. For electricity metering, the standards listed in following table should be taken into consideration:

Table 12 - Standards for electricity metering

Organisation	Reference	Title
Cenelec	EN 50470-1:2006	Electricity metering equipment (a.c.) — Part 1: General requirements, tests and test conditions — Metering equipment (class indexes A, B and C)
Cenelec	EN 50470-3:2006	Electricity metering equipment (a.c.) — Part 3: Particular requirements — Static meters for active energy (class indexes A, B and C)
Cenelec	EN 62052-11:2020	Electricity metering equipment - General requirements, tests and test conditions - Part 11: Metering equipment
Cenelec	EN 62053-24:2020[17]	Electricity metering equipment - Particular requirements - Part 24: Static meters for fundamental component reactive energy (classes 0,5S, 1S, 1, 2 and 3)

The complete list of standards relevant to the MID can be found on the European Commission MID website[18]. The implementation of this directive is closely related with WELMEC (Western European Legal Metrology Cooperation). Together with the European Commission, guidance documents ensure coherent application of MID. The guidance documents are a not a legally binding interpretation of the directive. The legally binding text remains that of relevant Directives. An example of a guidance document can be found in the link in the footnotes.[19]

- WELMEC 7.2 2020 Software Guide (Measuring Instruments Directive 2014/32/EU)

Normative documents by OIML (Organisation Internationale de la Métrologie Légale) may be identified as giving presumption of conformity with the essential requirements of the MID. Active electrical energy meters - OIML R 46, 2012 - 2014/32/EU MI-003 is the normative document by OIML that applies to electricity metering.[20]

Complete lists of guidance and normative documents can be found at the following links:

- https://www.welmec.org/guides-and-publications/guides/
- https://www.oiml.org

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0032

[17] EU harmonised standards have no reference related to reactive power measurements. Since reactive power is essential component in management power networks, we see measurement of reactive component as essential requirement of any electricity smart meter.

[18] https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/measuring-instruments_en

[19] https://www.welmec.org/guides-and-publications/guides/#panel-5520-7-2

[20] https://www.oiml.org/en/files/pdf_r/r046-1-2-e12.pdf

5.1.2 Electromagnetic compatibility directive (EMCD)

The electromagnetic compatibility directive (EMCD, Directive 2014/30/EU)[21] ensures that electrical and electronic equipment does not generate, or is not affected by, electromagnetic disturbance. EMCD's topic is complex. Many relevant standards have cross-references to each other or are included in other topics. As an example, general requirements for electricity metering devices EN 50470-1:2007/A1 :2019 has the following additional standards not included in EMCD (the list in Table 13 is not complete).

Table 13 - Standards relevant to the electromagnetic compatibility directive

Organisation	Reference	Title
Cenelec	EN 61000-4-2:2009	Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test (/EC 61000-4-2:2008)
Cenelec	EN 61000-4-3:2006, +A 1 :2008 +A2:2010	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test
Cenelec	EN 61000-4-4:2012	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test (/EC 61000-4-4:2012)
Cenelec	EN 61000-4-5:2014	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test (/EC 61000-4-5:2014)
Cenelec	EN 61000-4-6:2014	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances induced by radio-frequency fields (/EC 61000-4-6:2013)
Cenelec	EN 61000-4-8:2010	Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity (/EC 61000-4-8:2009)
Cenelec	EN 61000-4-12:2006	Electromagnetic compatibility (EMC) - Part 4-12: Testing and measurement techniques - Oscillatory waves immunity test (/EC 61000-4-12:2006)

Due to that, the European Commission released the EMCD guide to assist with the common application on EMCD. A summary list of titles and references of harmonised standards can be found on the European Commission website. at the following link: https://ec.europa.eu/docsroom/documents/45365/attachments/1/translations/en/renditions/native

5.1.3 Low voltage directive (LVD)

The (LVD, Directive 2014/35/EU)[22] ensures that electrical equipment within certain voltage limits provides a high level of protection for European citizens, and benefits fully from the single market. It has been applicable since 20 April 2016.

The LVD covers health and safety risks on electrical equipment operating with an **input or output voltage** of between

- 50 and 1000 V for alternating current
- 75 and 1500 V for direct current

[21] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0030

[22] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0035

The general product safety directive (2001/95/EC)[23] covers consumer goods with a voltage below 50 V for alternating current, or below 75 V for direct current. It aims to ensure that only safe consumer products are sold in the EU.

Importantly, LVD does not cover voltages within equipment and does not cover individual electronic components. Also, very important information is the exclusion of certain equipment and standards due to reference in another topic. An example is EN 62052-31, which covers product safety specifics for electricity metering equipment (a.c.).

The European Commission issued an LVD guide[24] which explains various elements of the directive and its application. A more complete summary list of titles and references of harmonised standards can be found on the European Commission site:
https://ec.europa.eu/docsroom/documents/38783

5.1.4 Radio Equipment Directive

The radio equipment directive (RED, Directive 2014/53/EU)[25] establishes a regulatory framework for placing radio equipment on the market. It ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects. These include technical features against fraud and for the protection of privacy and personal data. Furthermore, additional aspects cover interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software.

Like EMCD and LVD, RED is very complex. For that purpose, the European Commission has put forward the RED Guide, which aims to help with the common application of the RED[26]. An extensive summarised list of harmonised standards can be found on the European Commission website at the following link:
https://ec.europa.eu/docsroom/documents/40222

5.1.5 Example list of technical standards in EU declaration of conformity

An example of a declaration of conformity would state that electricity meter type AM550-ED1[27] is in compliance with the following directives…:

- Directive on measuring instruments 2014/32/EU
- Electromagnetic Compatibility Directive 2014/30/EU
- Radio Equipment Directive 2014/53/EU

… and the following standards:

- EN 50470-1: 2006
- EN 50470-3: 2006
- EN 62059-32-1: 2012

[23] http://ec.europa.eu/consumers/consumers_safety/product_safety_legislation/index_en.htm

[24] https://ec.europa.eu/docsroom/documents/31221

[25] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053

[26] https://ec.europa.eu/docsroom/documents/29782

[27] Type designation: Advanced Metering (AM), Series (5), Family (50), Single phase: (-E), DIN connection 85A (1)

- IEC 62052-11: 2003
- IEC 62053-21: 2003
- CLC/TR50579: 2012
- EN 62368-1: 2014 + A11:2017
- EN 62311: 2008,
- EN 301 489-1: 2017,
- Draft EN 301 489-52: 2016
- EN 301 511: 2017
- EN 301 908-1: 2016
- EN 301 908-13: 2017

5.1.6 BRIGHT standards requirement

Based on the brief overview and on the example provided in the previous subsection, we can state that the general requirement for the BRIGHT project to follow in terms of standards is as follows:

SR: Ensure that smart metering devices have a declaration of conformity stating compliance with applicable EU directives and standards.

5.2 Legal requirements

In the section below, in addition to the analysis of legal framework covering privacy (Section 2) and cybersecurity (Section 3) we have reviewed EU-wide regulations and directives relevant to the energy market (*inter alia* Clean Energy Package). Legal frameworks regulating public sector energy actors are kept out of the analysis, which focuses only on private sector actors and their relationship with final costumers.

5.2.1 The path towards the Clean Energy Package

The terms “liberalisation” and “deregulation” became popular in the 1980s and have been used mainly to indicate markets’ opening through the progressive reduction of constraints on their operations and the removal of barriers to entry imposed by the public authorities.

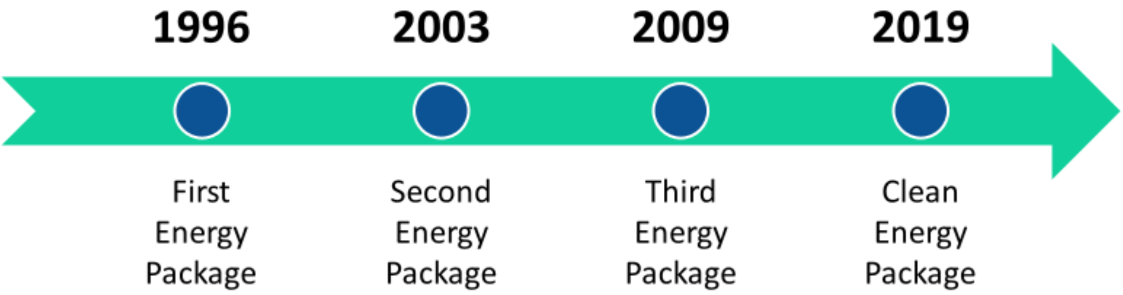
Formerly, the electricity flow was mainly unidirectional and energy supply was a natural monopoly spanning generation, distribution, and trading. Today, liberalisation has separated those steps in the supply chain and planned regulation schemes both for activities in which natural monopolies remain (typically transmission and distribution) and for competitive energy trading markets.[28]

European energy markets started to become liberalised in 1996 with the adoption of the First Energy Package (Pollitt, 2019). The Package set provisions for the liberalisation of the internal market for electricity and gas, aiming for management and accounting unbundling of Transmission System Operators (TSOs). The Second Energy Package, adopted in 2003, carried on the liberalisation of the internal market for electricity and gas, enabling industrial and domestic consumers to choose their gas and electricity suppliers freely thanks to the legal unbundling of TSOs. The Third Energy Package pursued the aim of further liberalising and integrating the internal energy markets by

[28] https://ec.europa.eu/energy/content/liberalisation-energy-market-electricity-and-gas_en

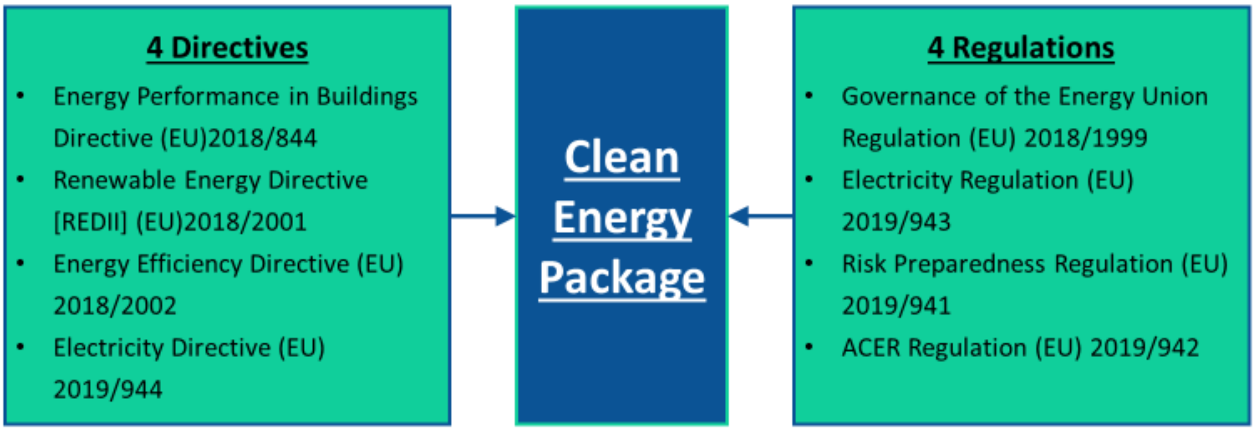
setting rules for opening and improving competition in retail markets (*What Does Liberalization and Unbundling of Energy Markets Mean?*, 2017).

Figure 13 - Timeline of EU energy market legislative packages



In the same way, the most recent Energy Package, also called the Clean Energy Package, was adopted by the European institutions between 2018 and 2019 with the aim of further liberalising energy markets. The Clean Energy Package focused attention on small energy consumers. It includes eight legislative texts - four directives and four regulations - on the electricity market and consumers, energy efficiency and the energy efficiency of buildings, renewables and bioenergy sustainability as well as governance of the Energy Union.

Figure 14 - The legislative composition of the Clean Energy Package



4 Directives

- Energy Performance in Buildings Directive (EU)2018/844
- Renewable Energy Directive [REDII] (EU)2018/2001
- Energy Efficiency Directive (EU) 2018/2002
- Electricity Directive (EU) 2019/944

Clean Energy Package

4 Regulations

- Governance of the Energy Union Regulation (EU) 2018/1999
- Electricity Regulation (EU) 2019/943
- Risk Preparedness Regulation (EU) 2019/941
- ACER Regulation (EU) 2019/942

As mentioned above, the focus of the first three energy packages was on building a common European energy market. In other words, all these packages had a macro focus and to some degree ignored households, small and medium-sized enterprises, and other small-scale energy consumers, who have only recently begun to receive legislative attention. Part of this shift can be further summarized as follows: while former regulations focused on consumers as passive subjects requiring protection, newer regulations view consumers as active marketagents .

This shift started with the 2012/27/EU Directive on energy efficiency, in which energy consumers were defined as active participants. Article 15, paragraph 8 of the Directive recites: "*Member States shall ensure that national energy regulatory authorities encourage demand side resources, such as demand response, to participate alongside supply in wholesale and retail markets*."

New regulations also foresee more detailed definitions of the demand-side of energy markets. This more substantial categorisation is summarized in the following sections.

5.2.1.1 Prosumers

The new rules about consumer rights and actors are held in the Electricity Directive (EU) 2019/944, in the Electricity Regulation (EU) 2019/943, as well as in some complementary parts of Directive (EU) 2018/2001 (RED II).

The number of prosumers has been increasing in Europe. As mentioned in D3.1, prosumers are consumers who also produce energy, at times if not always. Although prosumers also produce energy, they continue to be protected under the rights of passive consumers under EU law (*Prosumer Rights: Options for an EU Legal Post-2020*, 2016). Conversely, the European Parliament claims that a legal definition that distinguishes prosumers from other market actors is necessary; said language is yet to be developed (*Electricity "Prosumers,"* 2016). A European Commission report (*Energy Communities*, 2020) called "Mainstreaming RES" makes a (non-legal) definition of "self-generation" and"self-consumption". "Self-generation" implies that a generation unit (e.g. a PV module) produces electricity on-site, fed into the grid. When this electricity is (partly) consumed on-site, it is considered self-consumption.

Currently, individual self-consumption is possible in most Member States (*Regulatory Aspects of Self- Consumption and Energy Communities*, 2019). Nevertheless, legal, administrative, and market barriers still exist.

While RED II deals with the legal and administrative barriers for self-consumption, the Electricity Directive (EU) 2019/944, complemented by the Electricity Regulation (EU) 2019/943, approaches market-related barriers to self-consumption. Together, the Red II and the Electricity Directive (EU) 2019/944 intend to establish better conditions for self-consumption. In order to do so Directive (EU) 2019/944 provides an alternative definition of self-consumers, dubbing them "active customers". The Directive states that active consumers can participate in wholesale markets to purchase electricity for their own use and sell their self-generated electricity. However, it should not be their main business activity.This definition of active customer in Directive (EU) 2019/944 is more comprehensive than the definition of self-consumer in RED II, because it includes activities such as the participation in flexibility or energy efficiency schemes and covers the jointly acting final customers. Article 2, paragraph 8 of the Directive (EU) 2019/944 defines active customers as a "*final customer, or a group of jointly acting final customers, who consumes or stores electricity generated within its premises located within confined boundaries or, where permitted by a Member State, within other premises, or who sells self-generated electricity or participates in flexibility or energy efficiency schemes, provided that those activities do not constitute its primary commercial or professional activity*."

According to Article 15, paragraph 3 of the same Directive, Member States may adopt different provisions for the individual and jointly acting active customers but any different treatment for jointly acting active customers is to be proportionate and duly justified.

5.2.1.2 Aggregators and Demand Response

Making electricity consumption more flexible is one way to achieve cleaner, more secure, and more efficient electricity. Adjusting electricity consumption in order to reduce peaks in demand or take advantage of renewable sources is often described as "demand-side flexibility" (Malizou, 2018).

DR is the set of technical and technological solutions for ameliorating energy system flexibility. It is a time-based change in end-user's energy consumption and/or generation due to a reaction to price signals or by other measures (Stluka et al., 2018).

Directive (EU) 2019/944, which amends the Directive (UE) 2012/27/EU, defines DR as "*the change of electricity load by final customers from their normal or current consumption patterns in response to market signals, including in response to time-variable electricity prices or incentive payments, or* *in response to the acceptance of the final customer's bid to sell demand reduction or increase at a price in an organised market [...] whether alone or through aggregation*".

An "aggregator" is a new type of energy service provider that can increase or reduce the electricity consumption of a group of consumers according to the total electricity demand on the grid. An aggregator can also operate on behalf of a group of consumers producing their own electricity by selling excess electricity (Malizou, 2018).

Article 13, paragraph 1 of the Electricity Directive (EU) 2019/944 says that: "*Member States shall ensure that all customers are free to purchase and sell electricity services, including aggregation, other than supply, independently from their electricity supply contract and from an electricity undertaking of their choice*" and when the final customer wants to conclude an aggregation contract is entitled to do so without the consent of the final customer's electricity undertakings (Article 13, paragraph 2). In addition, Member States must establish an obligation for the aggregators in order to fully inform customers. Aggregators must also communicate to their customers, upon request, "*all relevant demand response data or data on supplied and sold electricity free of charge at least once every billing period*." Lastly, Member States must ensure that customers are not treated in a discriminatory way with regard to technical and administrative procedures or charges by their supplier if they opt for a contract with an independent aggregator.

The precepts regarding independent aggregators' market participation are set out in Article 17 of the Directive, which states that Member States must allow and foster DR participation through aggregation in all electricity markets. TSOs and DSOs must conduct non-discriminatory behaviour towards market participants engaging in DR aggregation when procuring ancillary services.

According to paragraph 3 of Article 17, Member States must ensure that their relevant regulatory frameworks include at least the following elements:

- rights for aggregators (including independent aggregators) to enter all electricity markets, without the consent of other market participants;
- non-discriminatory and transparent rules for the roles and responsibilities of all undertakings and customers, as well as the procedures for the exchange of data between aggregators and other electricity undertakings;
- an obligation for aggregators to be financially responsible for the imbalances that they cause: they must be Balance Responsible Party (BRP) themselves or delegate this responsibility, following Article 5 of Regulation (EU) 2019/943;
- a provision preventing suppliers from charging final customers undue payments, or penalties if they contract with an independent aggregator;
- a conflict resolution mechanism between aggregators and other market participants that includes responsibility for imbalances.

Article 17, paragraph 4 adds that "*Member States may require electricity undertakings or participating final customers to pay financial compensation to other market participants or to the market participants' balance responsible parties, if those market participants or balance responsible parties are directly affected by demand response activation*."

In order to introduce flexibility and energy efficiency, the smart metering system has to be implemented. It enables consumers to take effective control of their consumption.

Both the Electricity Directive 2009/72/EC and the Energy Efficiency Directive 2012/27/EU obliged Member States to install smart meters. Annex I of the Electricity Directive 2009/72/EC required Member States to install smart meters in 80% of consumers by 2020, if positively assessed in a cost-benefit analysis (CBA). Based on an analysis of a 2020 ACER and CEER report (*ACER Market Monitoring Report 2019 – Energy Retail and Consumer Protection Volume*, 2020), Nouicer et al. found that only nine countries had reached the 80% target by the end of 2019: Spain, Italy, Malta, Luxembourg, Denmark, Estonia, Norway, Sweden and Finland (Nouicer et al., 2020). Italy is already rolling out the second generation of smart meters, and Finland and Sweden are planning to do so. More than half of the Member States reached a 10% roll-out. However, some Member States postponed their 80% roll-out target to a later date.

Directive (EU) 2019/944 identifies smart metering as a fundamental technology for consumer engagement. Article 2, paragraph 23 defines smart metering as "*an electronic system that is capable of measuring electricity fed into the grid or electricity consumed from the grid, providing more information than a conventional meter, and that is capable of transmitting and receiving data for information, monitoring and control purposes, using a form of electronic communication*."

As we can note, the definition includes the functionality of measuring the electricity injected into the grid.

Article 19, paragraph 2 adds that "*Member States shall ensure the deployment in their territories of smart metering systems that assist the active participation of customers in the electricity mark et. Such deployment may be subject to a cost-benefit assessment which shall be undertaken in accordance with the principles laid down in Annex II*."

According to Annex II, the Member State or the designated competent authority must prepare a timetable with a target for up to 10 years for the deployment of smart metering.

5.2.1.3 Energy Communities

Energy communities organise collective and citizen-driven energy actions in order to make ready clean energy transition.

Renewable Energy Communities (hereafter REC) prepare for a clean energy transition while moving citizens to the fore. They contribute to raise public acceptance of renewable energy projects and make it easier to attract private investments in the clean energy transition. Concurrently, they can provide direct benefits to citizens by advancing energy efficiency and reducing their electricity bills (*Energy Communities*, 2020).

Verde and Rossetto survey the legal literature on the REC legal forms (Verde & Rossetto, 2020). According to Roberts et al. REC communities in Europe differ from one another due to different legal national systems (Roberts et al., 2014). The following archetypal legal forms are identified:

- limited partnerships (typically with limited liability company as general partner);
- cooperatives;
- trusts and foundations;
- non-profit customer-owned enterprises;
- housing associations;
- other socially-oriented enterprises.

As mentioned in Section 4.5, a juridical form guarantees the community's ability to self-manage a common-pool resource without overusing it and within the established property rights. Cooperatives, for instance, are a natural legal form for CRE projects, as they usually combine shared ownership, democratic participation in decision-making, and social responsibility.

By supporting citizen participation, energy communities can help in providing flexibility to the electricity system through demand-response and storage.

Directive (EU) 2019/944 defines a **Citizen Energy Community** (hereafter CEC) as a legal entity that:

a) *"is based on voluntary and open participation and is effectively controlled by members or shareholders that are natural persons, local authorities, including municipalities, or small enterprises;*

b) *has for its primary purpose to provide environmental, economic or social community benefits to its members or shareholders or to the local areas where it operates rather than to generate financial profits; and*

c) *may engage in generation, including from renewable sources, distribution, supply, consumption, aggregation, energy storage, energy efficiency services or charging services for electric vehicles or provide other energy services to its members or shareholders*."

RECs and CECs are both voluntary and value-driven legal entities established with specific governance and controls. CEC activities are limited to the electricity sector but may include generation from non-Renewable Energy System and other non-generation activities.

According to Article 16 of Directive (EU) 2019/944, participation in a CEC should be open and voluntary; members or shareholders of a citizen energy community should be entitled to leave the community; members or shareholders of a citizen energy community should do not lose their rights and obligations as household customers or active customers; relevant distribution system operators should cooperate with citizen energy communities to facilitate electricity transfers within citizen energy communities; citizen energy communities should subject to non-discriminatory, fair, proportionate and transparent procedures and charges, including with respect to registration and licensing, and to transparent, non-discriminatory and cost-reflective network charges.

In addition, CECs should be able to access all electricity markets directly or through aggregation. They are not to face any discriminatory treatment concerning the different activities they may undertake, i.e., final customers or production, supply, system operation, or aggregation. Lastly, they should be entitled to share the electricity produced within the community without prejudice to their rights and obligations as final customers.

The Member States might decide that CECs are open to cross-border participation. They might also provide the right for CECs to own, manage, establish, purchase or lease the distribution network in their area of operation.

5.2.1.4 P2P trading

The Clean Energy Package contains many provisions for collective self-consumption and P2P trading. P2P trading platforms allow prosumers to exchange their self-generated (renewable) electricity with other prosumers or consumers. It is possible to find several P2P trading initiatives using different technologies. Blockchain is one of them and is used to certify energy transfers. A more clear regulation for these platforms is necessary (Benedettini et al., 2019). A new market design directive for the period 2025-2030 is also recommended in order to address emerging issues arising from P2P trading, virtual power plants and the flexibility services procurement at the distribution level (Benedettini et al., 2019).

RED II Directive provides the right for renewables self-consumers to engage in P2P energy trading. According to Article 21, paragraph 2 of RED II, renewables self-consumers, individually or through aggregators, can sell their excess production of renewable electricity to electricity suppliers through renewables power purchase agreements and P2P trading arrangements. P2P trading of renewable energy is the sale of renewable energy between market participants (Article 2, paragraph 18 of RED II).

RED II Directive defines P2P trading of renewable energy as "*the sale of renewable energy between market participants by means of a contract with pre-determined conditions governing the automated execution and settlement of the transaction, either directly between market participants or indirectly through a certified third-party market participant, such as an aggregator. The right to conduct peer-to-peer trading shall be without prejudice to the rights and obligations of the parties involved as final customers, producers, suppliers or aggregators;*"

Generally, the RED II enables a range of market participants to engage in P2P trading of renewable energy (no restriction about the type of customer). Some issues could be caused when green and grey electricity are mixed, e.g. in a storage unit.

Besides, P2P energy trading can take place directly between market participants. Alternatively, this activity may be outsourced to a third party, such as an aggregator. In this case, this third party must be certified under conditions to be set by the Member States.

5.2.2 BRIGHT legal requirements

Given the definitions and categorisations provided by the European legal framework and summarised above, we can now proceed to provide the legal requirements for the BRIGHT project.

LR1. BRIGHT should guarantee citizen energy communities are subject to non-discriminatory, fair, proportionate, and transparent procedures and charges.

LR2. BRIGHT should ensure that any CECs involved are able to access all electricity markets directly or through aggregation.

LR3. In order to develop P2P energy trading by smart contracts, BRIGHT has to follow the definition of smart contract provided within the RED II Directive: "[a] *contract with pre-determined conditions governing the automated execution and settlement of the transaction, either directly between market participants or indirectly through a certified third-party market participant, such as an aggregator. The right to conduct peer-to-peer trading shall be without prejudice to the rights and obligations of the parties involved as final customers, producers, suppliers or aggregators*".

6 Conclusions

This document has presented requirements connected to privacy, ethics, and legal concerns. The requirements are both prescriptive (those related to privacy and legal aspects) and highly suggested (those related to ethics concerns). BRIGHT as a whole will benefit from the adherence to these requirements since they aid in avoiding or mitigating specific concerns and in crafting a virtuous and substantiated image of the project. The adherence to the requirements and their significance to consumers, citizens, and communities will be measured through diverse techniques ranging from internal evaluations to the field research.

6.1 Relation to other Work Packages and Tasks

The work presented herein, therefore, is pivotal for the BRIGHT project. Specifically, it affects the following workpackages and tasks in the ways described in each bullet.

- WP1
  - T1.3 – aids in the development of future versions of the Data Management Plan
  - T1.4 – aids in Privacy and Ethics Compliance Monitoring.
- WP3
  - T3.3 – provides portions of the benchmark for the assessment and evaluation of citizen engagement strategies and social acceptance of DR programs.
- WP4
  - T4.1 – provides portion of the framework for the Scalable privacy-preserving Data Collection.
- WP7
  - T7.3, T7.4, T7.5, T7.6 – provides privacy, ethical, and legal requirements to be measured and validated in pilots.
- WP8
  - T8.5: this deliverable may be used a starting point for any gap analyses performed in relation to standardization research and activities.

6.2 Relation to National Recovery and Resilience Plans

As a final note, the authors of this document wish to imprint on partners the importance of monitoring the evolution of the implementation of their country's National Recovery and Resilience Plan (NRRP) as it pertain to DR technologies. A comparative analysis of the plans would have been out of scope for this deliverable, but it seemed necessary to include this post-scriptum in an attempt to steer attention towards them. Indeed, a good portion of some, if not all, of the plans is directed at encouraging adoption of innovations with positive environmental impact, something that DR can favour. From a preliminary analysis, it can be said that some countries present energy-specific sections (also known as "missions" in some policy documents) of their NRRP, sections which are of indubitable consequence for BRIGHT consortium partners.

For a complete list of the EU27's NRRPs, partners can consult the following link:
https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en#national-recovery-and-resilience-plans

References

1. *A European Green Deal: Striving to be the first climate-neutral continent*. (2019). https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en
2. *ACER Market Monitoring Report 2019 – Energy Retail and Consumer Protection Volume*. (2020). https://www.acer.europa.eu/Official_documents/Acts_of_the_Agency/Publication/ACER
3. *Appropriate security measures for smart grids Guidelines to assess the sophistication of security measures implementation*. (2012). https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids
4. *Article 29 Working Party Opinion on Anonymisation Techniques*. (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
5. *Assessing the U.S. Climate in February 2021*. (2021). https://www.ncei.noaa.gov/news/national-climate-202102
6. Åström, K. J., & Murray, R. (2021). *Feedback Systems: An Introduction for Scientists and Engineers* (2nd ed.). Princeton University Press.
7. Benedettini, S., Brugnetta, G., Fumiatti, F., Gentili, P., Ghiglione, G., Giordano, V., Gidron, A., Küpper, G., Mandatova, P., Masci, R., Rubino, A., & Rubino. (2019). *Assessment and Roadmap for the Digital Transformation of the Energy Sector towards an Innovative Internal Energy Market*. https://www.euneighbours.eu/sites/default/files/publications/2020- 03/MJ0220185ENN.en_.pdf.
8. Brey, P. (2013). Ethics of Emerging Technologies. In S. O. Hansson (Ed.), *Methods for the Ethics of Technology* (pp. 175–192). Rowman and Littlefield International. https://research.utwente.nl/en/publications/ethics-of-emerging-technologies
9. Butun, I., Lekidis, A., & Santos, D. (2020). Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities. *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, 733–741. https://doi.org/10.5220/0009187307330741
10. Chen, J. (2021). *Environmental, Social, and Governance (ESG) Criteria*. Investopedia. https://www.investopedia.com/terms/e/environmental-social-and-governance-esg-criteria.asp
11. Ciscar, J. C., Feyen, L., Soria, A., Lavalle, C., Raes, F., Perry, M., Nemry, F., Demirel, H., Rozsai, M., Dosio, A., Donatelli, M., Srivastava, A., Fumagalli, D., Niemeyer, S., Shrestha, S., Ciaian, P., Himics, M., Doorslaer, B., Barrios, S., & Ibarreta, D. (2014). *Climate impacts in Europe - The JRC PESETA II project*. https://doi.org/10.2791/7409
12. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. (2013). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001
13. de Villiers, C., & Dimes, R. (2021). Determinants, mechanisms and consequences of corporate governance reporting: a research framework. *Journal of Management and Governance*, *25*(1), 7–26. https://doi.org/10.1007/s10997-020-09530-0
14. *Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944
15. *Electricity "Prosumers."* (2016). https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)593518
16. *Energy communities*. (2020). https://ec.europa.eu/energy/topics/markets-and-consumers/energy-communities_en
17. *Ethics Guidelines for Trustworthy AI*. (2019). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419
18. *EU Energy Poverty Observatory*. (2021). https://www.energypoverty.eu/
19. *European Social Policy Network Report*. (2018).
20. *Extreme Cold & Winter Update #1*. (2021).
21. *Fattori di emissione atmosferica di gas a effetto serra nel settore elettrico nazionale e nei principali paesi europei*. (2020).
22. Francesco, F. De, & Guaschino, E. (2020). Reframing knowledge: A comparison of OECD and World Bank

discourse on public governance reform. *Policy and Society*, *39*(1), 113–128. https://doi.org/10.1080/14494035.2019.1609391

23. García Alvarez, G., & Tol, R. (2020). *The Impact of the Bono Social de Electricidad on Energy Poverty in Spain*. https://econpapers.repec.org/RePEc:sus:susewp:0420
24. Großmann, K., & Kahlheber, A. (2017). Energy poverty in an intersectional perspective. In N. Simcock, H. Thomson, S. Petrova, & S. Bouzarovski (Eds.), *Energy Poverty and Vulnerability* (1st ed., p. 21). Taylor & Francis. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315231518-2/energy-poverty-intersectional-perspective-katrin-großmann-antje-kahlheber
25. *Guidelines for smart grid cybersecurity*. (2014). https://doi.org/10.6028/NIST.IR.7628r1
26. *Guidelines on notification of Operators of Essential Services incidents – Formats and procedures*. (2018). http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677
27. Hall, S., Jonas, A. E., Shepherd, S., & Wadud, Z. (2019). The smart grid as commons: Exploring alternatives to infrastructure financialisation. *Urban Studies*, *56*(7), 1386–1403. https://doi.org/10.1177/0042098018784146
28. Hristov, P., & Dimitrov, W. (2018). *The blockchain as a backbone of GDPR compliant frameworks*.
29. Kelly, S., Mclaughlin, T., & Verma, S. (2021, May 16). Explainer: Texas's one-of-a-kind power system raises questions during price spike. *Reuters*. https://www.reuters.com/business/energy/texass-one-of-a-kind-power-system-raises-questions-during-price-spike-2021-02-16/
30. Malizou, A. (2018). *Electricity Aggregators: Starting off on the Right Foot with Consumers*. https://www.beuc.eu/publications/beuc-x-2018-010_electricity_aggregators_starting_off_on_the_right_foot_with_consumers.pdf
31. Michel, J. D., & Walden, I. (2018). *How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive*. *Queen Mary*(291).
32. Mill, J. S. (1844). On the Definition of Political Economy. In *The Collected Works of John Stuart Mill, Vol. IV*. University of Toronto Press. https://www.routledge.com/Collected-Works-of-John-Stuart-Mill-IV-Essays-on-Economics-and-Society/Robson/p/book/9780415604758
33. Moriarty, J. (2021). Business Ethics. In *The Stanford Encyclopedia of Philosophy* (Summer 202). https://plato.stanford.edu/entries/ethics-business
34. Mrabet, Z. El, Ghazi, H. El, Kaabouch, N., & Ghazi, H. El. (2018). *Cyber-Security in Smart Grid: Survey and Challenges*. https://doi.org/10.1016/j.compeleceng.2018.01.015
35. Nouicer, A., Kehoe, A.-M., Nysten, J., Fouquet, D., Hancher, L., & Meeus, L. (2020). *The EU clean energy package (ed. 2020)*. https://doi.org/10.2870/58299
36. Ostrom, E. (2005). *Understanding Institutional Diversity*. Princeton University Press.
37. Patrucco, D. (2020, December 22). No Title. Quale Energia. https://www.qualenergia.it/articoli/magliano-alpi-nuova-comunita-energetica-sotto-albero-di-natale/
38. Pollitt, M. G. (2019). The European Single Market in Electricity: An Economic Assessment. *Review of Industrial Organization*, *55*(1), 63–87. https://doi.org/10.1007/s11151-019-09682-w
39. *Privacy and Data Protection by Design*. (2015). https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
40. *Proposal for a Regulation on a European Approach for Artificial Intelligence*. (2021).
41. *Prosumer rights: Options for an EU legal post-2020*. (2016). https://www.documents.clientearth.org/wp-content/uploads/library/2016-05-01-prosumer-rights-options-for-an-eu-legal-framework-post-2020-ce-en.pdf
42. Rademakers, K., Smith, M., Yearwood, J., Saheb, Y., Moerenhout, J., Pollier, K., Debrosses, N., Badouard, T., Peffen, A., Pollitt, H., Heald, S., & Altmann, M. (2018). *Study on Energy Prices, Costs and Subsidies and their Impact on Industry and Households*. https://doi.org/10.2833/825966
43. *Reference document on security measures for Operators of Essential Services*. (2018). https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf
44. *REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52*. https://eur-

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

45. *Regulatory Aspects of Self- Consumption and Energy Communities*. (2019). https://www.ceer.eu/documents/104400/-/-/8ee38e61-a802-bd6f-db27-4fb61aa6eb6a
46. Roberts, J., Bodman, F., & Rybski, R. (2014). *Community power: model legal frameworks for citizenowned renewable energy*. https://friendsoftheearth.eu/publication/model-legal-frameworks-for-citizen-owned-renewable-energy/
47. Searcey, D. (2021, May 3). No, Windfarms are not the Cause of the Texas Blackouts. *New York Times*. https://www.nytimes.com/2021/02/17/climate/texas-blackouts-disinformation.html
48. Sim, W. L., Chua, H. N., & Tahir, M. (2019). Blockchain for Identity Management: The Implications to Personal Data Protection. *2019 IEEE Conference on Application, Information and Network Security (AINS)*, 30–35. https://doi.org/10.1109/AINS47559.2019.8968708
49. Simon, H. (1957). *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization* (2nd ed.). Macmillan.
50. *Smart Grid Reference Architecture*. (2012). https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf
51. *Smart Grid Security: Recommendations for Europe and Member States*. (n.d.).
52. Smil, V. (2018). *Energy and Civilization*. MIT Press.
53. Stluka, P., Noyé, S., Anton, M. A., Tsagkrasoulis, D., & Konsman, M. J. (2018). *Analysis of EU-wide interoperability standards and data models and harmonization requirements*. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b9a42214&appId=PPGMS
54. Suhr, A., Rosinger, C., & Honecker, H. (2013). System Design and Architecture - Essential Functional Requirements vs. ICT Security in the energy domain. *International ETG-Congress 2013; Symposium 1: Security in Critical Infrastructures Today*, 1–9.
55. Tavani, H. T. (2015). *Ethics and technology : controversies, questions, and strategies for ethical computing* (5th ed.). Wiley and Blackwell. https://www.wiley.com/en-us/Ethics+and+Technology%3A+Controversies%2C+Questions%2C+and+Strategies+for+Ethical+Computing%2C+5th+Edition-p-9781119186571
56. *The EU Blockchain Observatory and Forum*. (2018). https://www.eublockchainforum.eu/
57. Uslar, M., Rosinger, C., & Schlegel, S. (2014). Security by Design for the Smart Grid: Combining the SGAM and NISTIR 7628. *2014 IEEE 38th International Computer Software and Applications Conference Workshops*, 110–115. https://doi.org/10.1109/COMPSACW.2014.23
58. Uslar, M., Schmedes, T., Lucks, A., Luhmann, T., Winkels, L., & Appelrat, H.-J. (2005). *Interaction of EMS Related Systems by Using the CIM Standard.* 596–610.
59. van de Poel, I., Royakkers, L., Verbeek, P.-P., & Brumsen, M. (2011). Ethics, technology and engineering: an introduction. In *Wiley-Blackwell, a John Wiley & Sons, Ltd., Publication* (Wiley and). https://www.wiley.com/en-us/Ethics%2C+Technology%2C+and+Engineering%3A+An+Introduction-p-9781444330953
60. Verde, S., & Rossetto, N. (2020). *The Future of Renewale Energy Communities in the EU*. https://doi.org/10.2870/754736
61. Weber, P. J., & Stengle, J. (2021, March 26). Texas death toll from February storm, outages surpasses 100. *AP News*. https://apnews.com/article/hypothermia-health-storms-power-outages-texas-ffeb5d49e1b43032ffdc93ea9d7cfa5f
62. Weiss, J., Levine, S. H., Sergici, S., & Thapa, A. (2018). *Demand Response for Natural Gas Distribution*. https://brattlefiles.blob.core.windows.net/files/13929_demand_response_for_natural_gas_distribution.pdf
63. *What does Liberalization and Unbundling of Energy Markets mean?* (2017). https://www.next-kraftwerke.com/knowledge/liberalization-energy-markets

Annex 1 – Full list of BRIGHT Privacy, Ethics, and Legal Requirements

The following table recaps the full set of Privacy, Ethics, and Legal Requirements (PELRs) for the BRIGHT project and provides a short description for each one.

Table 14 - List of BRIGHT PEL requirements

ID#	Requirement #	Description
PELR1	PMR	Documents supplied within the confines of WP10 guarantee the Privacy and data protection macrorequirement: compliance with GDPR.
PELR2	SMR	Demonstrate compliance with NISD, Cybersecurity Act, and state-of-the-art technical measures.
PELR3	ER1	The BRIGHT project should make a sufficient effort to represent replicability recommendations as empirical and not scientific.
PELR4	ER2	BRIGHT puts in place the requirements set by the EU proposal on AI regulation.
PELR5	ER3	BRIGHT considers that under the conditions specified in Annex III of the Commission's proposed regulations, its AI algorithm might be viewed as high-risk.
PELR6	ER4	BRIGHT makes an effective effort to forecast the possibile issues of fairness in the DR program and in the blockchain technology.
PELR7	ER5	BRIGHT puts in place communication efforts towards the pilot participants that enhance the social acceptability of the technologies implemented. These communication strategies will include, but not limited to, online and physical means and should aim to correctly communicate the ways to use the technologies implemented in the pilots, in order to avoid false expectations.
PELR8	ER6	BRIGHT should show whether the technologies used in the project contribute to reducing negative environmental impacts.
PELR9	ER7	BRIGHT should assess whether the environmental dimension is relevant in motivating consumers' choices to adopt DR solutions.
PELR10	ER8	BRIGHT communicates to individuals participating in local energy communities their rights with respect to any resource that can be considered common-pool.
PELR11	ER9	BRIGHT defines all seven rules governing interactions as they apply to each of the pilots, with special focus on the pemissible information exchanges, choices, and payoffs.
PELR12	ER10	In each of the pilots, BRIGHT takes into account pilot participants' feedback in establishing outcomes that are mutually agreed upon.
PELR13	ER11	BRIGHT technical partners assess whether DR solutions tested in the project could increase resilience to extreme weather events.
PELR14	ER12	BRIGHT consortium partners in charge of pilots offer low-cost IoT solutions, which can offer high cost-effectiveness, considering that the initial investment cost can be covered during the first year of application.
PELR15	ER13	BRIGHT consortium partners in charge of pilots might include individuals vulnerable to energy poverty in their samples in order to assesses whether these consumers perceive the project's technology mixes as useful to reducing energy poverty.
PELR16	SR	Ensure that smart metering devices have a declaration of conformity stating compliance with applicable EU directives and standards.
PELR17	LR1	BRIGHT should guarantee citizen energy communities are subject to non-discriminatory, fair, proportionate, and transparent procedures and charges.
PELR18	LR2	BRIGHT should ensure that any CECs involved are able to access all electricity markets directly or through aggregation.
PELR19	LR3	In order to develop P2P energy trading by smart contracts, BRIGHT has to follow the definition of smart contract provided within the RED II Directive: "[a] contract with pre-determined conditions governing the automated execution and settlement of the transaction, either directly between market participants or indirectly through a certified third-party market participant, such as an aggregator. The right to conduct peer-to-peer trading shall be without prejudice to the rights and obligations of the parties involved as final customers, producers, suppliers or aggregators".