Grant Agreement N° 872592

PLATOON

Digital platform and analytic tools for energy

Deliverable D1.4
Report on Legal & Ethics requirements

Contractual delivery date:
M6
Actual delivery date:
15/07/2020
Responsible partner:
P15: Mandat International, Switzerland

Project Title	PLATOON – Digital platform and analytic tools for energy
Deliverable number	D1.4
Deliverable title	Report on Legal & Ethics requirements
Author(s):	Adrian Quesada Rodriguez (MI), Renáta Radócz (MI), Sébastien Ziegler (MI)
Responsible Partner:	P15 – Mandat International
Date:	30/06/2020
Nature	R
Distribution level (CO, PU):	PU
Work package number	WP1 – Energy System Management Challenges
Work package leader	ENGIE, France
Abstract:	This report presents the initial evaluation of the legal and ethics requirements that are relevant to the PLATOON project. It performs a high-level personal data protection assessment for all PLATOON High/Low-level use-cases, enablers, and solutions, and presents general guidelines on GDPR compliance based on the functional requirements and overall specifications defined throughout PLATOON WP1
Keyword List:	Ethics, GDPR, Personal Data Protection, Guidelines, Requirements

The research leading to these results has received funding from the European Community's Horizon 2020 Work Programme (H2020) under grant agreement no 872592.

This report reflects the views only of the authors and does not represent the opinion of the European Commission, and the European Commission is not responsible or liable for any use that may be made of the information contained therein.

Editor(s):	Adrian Quesada Rodriguez (MI)
Contributor(s):	Valeria Di Pasquale (Poste Italiane); Valentina Janev (Institute Pupin); Maciej Gruszczyński (Fundingbox), Krystyna Stasiak (Fundingbox); Pau Joan Cortés Forteza (SAMPOL); Patrick Maurelli (UNIROMA); Gorka Naveran Lanz (VEOLIA)
Reviewer(s):	Philippe Calvez (ENGIE) – PLATOON Coordinator Erik Maqueda (TECN) – Technical Coordinator
Approved by:	Philippe Calvez (ENGIE) – PLATOON Coordinator Erik Maqueda (TECN) – Technical Coordinator Eduardo Jimenez (IND) – Exploitation Coordinator
Recommended Readers:	All WPs

Document Description

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v. 0.4	10/05/2020	Initial draft submitted to partners	Adrian Quesada Rodriguez, Sébastien Ziegler
v. 0.7	11/06/2020	Partner inputs received	All pilot owners
v. 0.9	30/06/2020	Draft version submitted for internal review (MI)	Adrian Quesada Rodriguez
V1.0	13/07/2020	Draft version submitted for project review	Adrian Quesada Rodriguez, Renáta Radócz
V1.1	13/07/2020	Internal review completed; changes addressed.	Adrian Quesada Rodriguez, Renáta Radocz
V1.2	15/07/2020	Project review feedback addressed. Final version submitted.	Adrian Quesada Rodriguez

Table of Contents

List of Figures

List of Tables

Terms and abbreviations

GDPR	General Data Protection Regulation
EDPB	European Data Protection Board
PDP	Personal Data Protection
IDS	International Data Spaces
DPIA	Data Protection Impact Assessment
PUI	Persistent Unique Identifier
LoA	Level of Assurance
HLUC	High-Level Use-Case
LLUC	Low-Level Use-Case

Executive Summary

This report presents the results of PLATOON Task 1.5. It carries out an initial evaluation of the legal and ethics requirements that are relevant to the PLATOON project. It performs a high-level personal data protection assessment for all PLATOON High/Low-level use-cases, enablers, and solutions, presenting general guidelines on GDPR compliance based on the functional requirements identified in D1.2.

Based on the initial assessments performed in direct connection with the work performed with other Tasks in this work packages, to this point in the project, no critical issues can be identified in the PLATOON project and the envisioned ecosystem from either the Ethical or the Personal Data Protection perspectives. This assessment will be continuously updated throughout the upcoming work in task 3.5, which will also consider the general guidelines and recommendations noted throughout this document to evaluate and support compliance by all partners and associated stakeholders.

1 Introduction

The PLATOON H2020 project seeks to digitalize the energy sector by developing a new generation of digital solutions and products that will enable the energy sector to transit from the current centralized system, based on the use of mainly non-renewable energy sources (fossils' based), towards a more decentralized and distributed system and an energy mix using renewables sources or even relying on consumption and CO_2 footprint reduction with new extended digital capabilities.

The main objectives of the project are:

1. To enhance the role of the energy sector stakeholders to let them reliably, fairly and securely extract knowledge from their own data.
2. To foster new business models in the energy sector using digital technologies.
3. To enhance the multi-party cooperation between technology providers and data owners.
4. To contribute to the standardization of the energy management systems by assessing
5. whether current standards offer the proper roles interfaces to enable business processes, including new ones and identify where new standards may be needed.

PLATOON addresses the objectives in an integrated approach that will be demonstrated across different demonstration locations. 7 pilots in 5 different countries that provide real Energy Big Data cases. It proposes to build the solution based on existing European standards and initiatives for managing the pilots' data, for the access, models, interfaces, governance, and sovereignty. It also foresees to report back the results to the different standardization working groups. PLATOON will facilitate the technology transfer into the market by a well-established tendering process through Open Calls.

The PLATOON architecture and components are valuable for the different stakeholders of the energy sector value chain, starting from the electricity supplier, passing through the distributor, the aggregator, the ESCo until the End User. As such, the project seeks to reinforce the European efforts for modernization of the European electricity grid as it focuses the attention to new smart grids services through data knowledge exploitation.

In this context, compliance with Ethical and Personal Data Protection Requirements is a high relevance action to be performed throughout the project. This document showcases the results of Task 1.5, particularly towards the identification of ethical and personal data protection-related issues that might arise during the project, and seeks to define a set of baseline guidelines to be implemented by all project partners and associated stakeholders in response to the functional requirements specified by Deliverable 1.2. The outcomes of this Task will be considered, supported, and updated (whenever necessary) by Task 3.3 (Security and Privacy), 3.5 (Legal and Ethics Support) and 10.4 (Legal and knowledge management).

2 Legal and Ethical Frameworks

This section introduces the fundamental legal and ethical frameworks to be considered throughout the PLATOON project. These elements will serve as a baseline for upcoming compliance-related tasks in the project's lifecycle and will be updated, as necessary by PLATOON Task 3.5.

2.1 Regional Legal Frameworks

2.1.1 The General Data Protection Regulation (GDPR)

Regulation 679/2016 of the European Parliament, better known as the GDPR, is the main European Union regulatory framework in the field of personal data[1] protection. It was signed in 2016 as a successor to Directive 95/46/EC to prevent disparities between the Member States in terms of procedures and sanctions and, generally, to harmonize personal data protection in the European Union. It applies to data processing operations performed by a data controller or processor established in the European Union and, in specific circumstances[2], to data processing operations of personal data of a data subject performed by a data controller or processor not established in the European Union.

The GDPR is based on nine cornerstone principles, namely the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and accountability (GDPR, 2016, Art. 5). These principles inform all the provisions of the Regulation and translate into corresponding rights and obligations for data subjects, data controllers and data processors accordingly. Moreover, the GDPR calls for the adoption of pseudonymized processing operations whenever possible to strengthen data subjects' privacy and the security of collected information.

The Regulation details requirements for consent to data processing operations, with more stringent requirements for consent to processing operations relating to minors of age and regarding special categories of data. It vests data subjects with direct rights vis-à-vis data controllers and processors and establishes numerous obligations for data controllers and processors to ensure security and reliability of data processing operations.

Under the GDPR, data subjects have a broad set of rights over their personal data, including the right to be informed of its use; the right to access the data that is being compiled or processed; the right to request the rectification, erasure or restriction of processing of such data; the right to data portability; the right to object; and a series of rights in relation to automated decision making and profiling.

On the other hand, the GDPR sets specific obligations for data controllers and processors. The regulation requires them to adopt a Data Protection by Design and by Default approach (included but not limited to the introduction of technical and organizational security measures)[3], and obliges

[1] Personal data is defined as "any information that relates to an identified or identifiable living individual" meaning that any information that can be used to identify a person falls in the context of personal data, even if this has been de-identified, encrypted or pseudonymized. Personal data anonymized in such a way that the individual is not identifiable is no longer considered personal data.

[2] The Regulation applies to data controllers or processors not established in the European Union when the data processing activities are related to: "a) the offering of good or services to data subjects in the European Union, irrespective of whether a payment of such data subject is required; b) the monitoring of data subjects' behavior as far as their behavior take place within the European Union; c) places where European Union Member States' law applies by virtue of public international law" (GDPR, 2016, Art. 3).

[3] Article 25 provides obligations for the data controller about data protection by design and by default both in the form of appropriate technical and organizational measures and the necessary safeguards into the processing of the personal data following the data protection principles defined in Article 5 of GDPR Regulation.

them to keep records of their processing activities and it requires the performance of Data Protection Impact Assessments of data processing operations entailing high risks for data subjects' rights and freedoms. Importantly, the GDPR also details rules that data controllers and processors must implement when transferring personal data to countries outside the European Union and, particularly, to those countries which do not ensure an equivalent level of protection.

In the context of PLATOON, the dispositions of the GDPR and the complementary guidelines and recommendations made by the European Data Protection Board (EDPB)[4] and the National Supervisory Authorities must be considered as the main point of reference vis-à-vis data protection requirements. As will be detailed below, the overall range of PLATOON activities have been tailored to closely follow these requirements and will continue to do so through the adoption of personal data protection and ethics by default approach.

2.1.2 The Directive on Privacy and Electronic Communication (ePrivacy Directive) and the European Union Regulation on Privacy of Electronic Communication (ePrivacy Regulation)

The ePrivacy Directive, soon to be replaced by the ePrivacy Regulation, is the reference legal framework for electronic communication. Its objective was to establish minimum requirements for security and confidentiality of communication, protection of traffic and location data and protection of the end-user terminal equipment. Technology evolution and the entry into force of the GDPR made necessary updating the ePrivacy Directive into a Regulation. This should trigger the harmonization of the legal frameworks across the European Union and allow aligning protection standards in electronic communication with those in force for personal data through the GDPR. With respect to the GDPR, the ePrivacy Regulation will be considered *lex specialis* and it is expected to address further aspects of electronic communications networks that may affect rights and freedoms of data subjects. In fact, the rise of new technologies such as edge computing and smart meters requires clearer rules to meet these new challenges. In this sense, the ePrivacy Regulation is likely to also provide for rules in machine to machine communication, e.g. devices will not be allowed to transfer personal data without prior consent, and clarify the limits of processing of massive amounts of metadata (European Commission 2017; IONOS 2020). Additionally, the ePrivacy Regulation should also introduce stricter rules on the use of cookies and other tracking solutions, which is likely to affect data subject-facing solutions and services. As pointed out by the European Data Protection Board, the adoption of the ePrivacy Regulation "*is necessary to ensure an even playing field and legal certainty for market operators*" (Andrea Jellinek 2019).

2.1.3 Directive on Security of Network and Information Systems (NIS Directive)

The NIS Directive constitutes the European Union legislation on cybersecurity and establishes the legal framework of the European Union in this field. It calls for the adoption of appropriate measures by the Member States to guarantee the security of the European Union's cyberspace. It covers all vital sectors in the economy and society, specifically those relying heavily on ICT systems. In this regard, businesses in these sectors that are identified by the Member States as operators of essential services are required to take appropriate security measures and to cooperate with national authorities for preserving the essential service (European Parliament, 2016, Recitals 4-6).

The purpose of the NIS Directive is to lay down measures to achieve a common level of security of network and information systems within the European Union. Security of network and information systems is defined as the ability to resist any action that affects the "*availability, authenticity, integrity*

[4] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems" (European Parliament, 2016, Art. 4(2)). The NIS Directive applies to two categories of entities: digital service providers and operators of essential services. Digital service providers are covered by the NIS Directive regime upon the sole transposition of the directive into Member States' national law. On the other hand, essential services are only covered by the scope of the NIS Directive upon designation as such by the respective Member State. In order to be considered essential, a service has to meet three cumulative criteria:

a) "*being considered essential for the maintenance of critical societal and economic activities;*

b) *being dependent upon network and information systems;*

c) *an incident would have significant disruptive effects on the provision of that service*" (European Parliament, 2016, Art. 5(2)).

2.1.4 Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)

The "eIDAS" Regulation was adopted by the European Union in 2014. It aims to offer a comprehensive legal framework across the Member States for mutual recognition and interoperation of cross-border eID management, trust services and certificates (European Council, 2014, Recital 2). Since the GDPR repealed Directive 95/46/EC, all provisions of the eIDAS Regulation should be interpreted and applied in accordance with the GDPR.

The eIDAS Regulation focuses on identification rather than authentication and specifies that its primary objective is the "unique identification" of a person (Tsakalakis et al., 2017, p. 33). The eIDAS Implementing Regulation 2015/1501 (R 2015/1501) clarifies that unanimous persons' identification takes place by transmitting a minimum dataset which should include a Persistent Unique Identifier (PUI). Moreover, the Regulation defines predetermined Level of Assurance (LoA) thresholds to guarantee the identity of services' users. There are three LoA levels:

- "Low" where evidence of identity is assumed to be valid (e.g. an account with a media service provider);
- "Substantial" where evidence has to be validated (e.g. services entailing online payments);
- "High" where evidence requires biometric validation (e.g. services linked to the use of electronic IDs) (Tsakalakis et al., 2017, p. 38).

2.2 Relevant European Data Protection Board Guidelines and National Laws

The following section showcases the relevant national dispositions and guidelines/recommendations set by the EDPB, which are to be considered when addressing personal data protection requirements throughout the PLATOON pilots and associated enablers. In the context of this deliverable and given the early stage of the pilots/ PLATOON enablers, the national requirements have been taken into account for the Data Protection Assessments found in Section 3.1.

Furthermore, the section will focus particularly on the EDPB guidelines on DPIA and the nationally defined lists of processing operations subject to a DPIA, which will be of relevance to showcase, at a high-level, the low-level of risk associated with the expected activities to be undertaken in PLATOON.

As part of its commitment to personal data protection and to maximize the potential for exploitation of the developed tools through the introduction of personal data protection by design and by default approach, the PLATOON project will perform continuous personal data protection compliance activities.

2.2.1 EDPB Guidelines:

The European Data Protection Board is an independent body which ensures that EU law in this field – especially the General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive – is consistently applied in all countries bound by them.

It promotes cooperation among the national data protection authorities, provides general guidance (including guidelines, recommendations, and best practice) to clarify the GDPR, adopts consistency findings, designed to make sure the GDPR is interpreted consistently by all national regulatory bodies, advises the European Commission on data protection issues and any proposed new EU legislation of particular importance for the protection of personal data, and encourages national data protection authorities to work together and share information and best practices with each other.

Relevant guidelines[5] for the PLATOON project include:

- Guidelines 05/2020 on consent under Regulation 2016/679
- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation
- Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation
- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation
- Guidelines on transparency under Regulation 2016/679, WP260 rev.01
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01
- Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01
- Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01
- Guidelines on Data Protection Officers ('DPO'), WP243 rev.01
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01

As noted by GDPR article 35: “Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.”.

The EDPB has clarified the situations where processing may result in a “high risk” in WP248 rev.01. where it has stated that “In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt”. As such the implementation of a DPIA can be considered to be necessary whenever two of the following criteria take place:

Activities requiring data protection impact assessment (EDPB)	**Taking place in PLATOON?**
1. Evaluation or scoring, including profiling and predicting, especially “from aspects concerning the data subject’s performance at work, economic situation, health,	No

[5] These guidelines shall be considered by all PLATOON partners throughout the implementation phases of the project.

personal preferences or interests, reliability or behaviour, location or movements" (recitals 71 and 91).	
2. Automated decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35 (3)(a)).	No
3. Systematic monitoring: processing used to observe, monitor, or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" (Article 35 (3)(c)).	No
4. Sensitive data: this includes special categories of data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offenses. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details.	No
5. Data processed on a large scale (determined based on 1. The number of data subjects concerned, either as a specific number or as a proportion of the relevant population. 2. The volume of data and/or the range of different data items being processed. 3. The duration, or permanence, of the data processing activity. 4. The geographical extent of the processing activity.)	No
6. Datasets that have been matched or combined, for example, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.	No
7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. (e.g. employees, children, patients, elderly, etc.).	No
8. Innovative use or applying technological or organizational solutions. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that use of a new technology can trigger the need to carry out a DPIA. This is because the use of a new technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore, require a DPIA.	Maybe (aggregated occupancy readings are taken in some pilots)
9. Data transfer across borders outside the European Union (recital 116), taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers, or the likelihood of transfers based on derogations for specific situations set forth by the GDPR.	No
10. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91)[6].	No

None of the envisioned PLATOON activities is likely to result in a high risk to the rights and freedoms of natural persons based on the criteria set by EDPB.

Table 1 Relevant EDPB Guidelines and DPIA Criteria

2.2.2 National Laws

The following table introduces a high-level overview of the national legislation on personal data protection that is applicable in each of the countries where PLATOON pilots are envisaged,

[6] This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or reusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database to decide whether to offer them a loan.

and which should be considered by the relevant partners during the implementation of PLATOON related activities.

For each country, an additional table is provided which showcases the nationally defined list of activities that are either subject or extent from Data Protection Impact Assessments as specified by the National Supervisory Authority. Whenever a national authority has specified only the cases exempt from the DPIA requirement, the EDPB guidelines listed in Section 2.2.1 take precedence in the determination of processing activities which require a DPIA.

<table>
<tr><th>Country</th><th>Relevant Personal Data Protection Legislation</th></tr>
<tr><td><b>Belgium</b></td><td>
<ul>
<li>Law relating to the protection of individuals with regard to the processing of personal data</li>
<li>Law establishing the information security committee and amending various laws concerning the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to processing personal data and the free movement of such data, and repealing Directive 95/46 / EC</li>
<li>Law establishing the Data Protection Authority</li>
<li>Law regulating the installation and use of surveillance cameras</li>
<li>List of processing operations requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679</li>
</ul>
<table>
<tr><th>Activities requiring data protection impact assessment (Belgium)</th><th>Taking place in PLATOON?</th></tr>
<tr><td>1) when the processing uses biometric data for the unique identification of data subjects in a public place or in a private place accessible to public;</td><td>No</td></tr>
<tr><td>2) when personal data is collected from third parties to be taken then taken into consideration as part of the decision to refuse or terminate a specific service with a natural person;</td><td>No</td></tr>
<tr><td>3) when the health data of a data subject is collected by automated means using an active implantable medical device;</td><td>No</td></tr>
<tr><td>4) when data is collected on a large scale from third parties to analyze or predict economic situation, health, personal preferences or interests, reliability or behavior, location, or movement of natural persons;</td><td>No</td></tr>
<tr><td>5) when particular categories of personal data within the meaning of Article 9 GDPR or data of a very personal nature (such as data on poverty, unemployment, the involvement of youth assistance or social work, data on domestic and private activities, location data) are exchanged systematically between several controllers;</td><td>No</td></tr>
<tr><td>6) when it comes to large-scale processing of personal data generated using devices with sensors that send personal data over the Internet or other means ("Internet of Things" applications, such as smart TVs, devices)</td><td>No</td></tr>
<tr><td>7) when it comes to large-scale and / or systematic processing of data telephony, Internet or other communication, metadata or location data of natural persons or allowing to lead to persons physical (for example Wi-Fi-tracking or processing location data from travelers on public transport) when processing is not strictly necessary for a service requested by the data subject;</td><td>No</td></tr>
</table>
</td></tr>
</table>

8) when it comes to large-scale personal data processing where the behavior of natural persons is observed, collected, established, or influenced, including for advertising purposes, and this systematically via automated processing.	No

None of the envisioned PLATOON activities is likely to result in a high risk to the rights and freedoms of natural persons based on the criteria set by the Belgian DPA.

France

- French Data Protection Act
- List of processing operations exempt from data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679

Activities exempt[7] from data protection impact assessments (France)	**Taking place in PLATOON?**
Treatments, implemented only for human resources purposes and under the conditions provided for by the applicable texts, for the sole management of the personnel of organizations which employ less than 250 people, with the exception of the use of profiling.	No
Supplier relationship management processes.	No
Treatments implemented under the conditions provided for by the texts relating to the management of the electoral register of the municipalities.	No
Treatments intended for the management of the activities of works and establishment committees.	No
Treatments implemented by an association, a foundation, or any other non-profit institution for the management of its members and donors in the framework of its usual activities as long as the data is not sensitive.	No
Processing of health data necessary for the care of a patient by a health professional practicing on an individual basis in a medical office, a pharmacy or a laboratory of medical biology.	No
Treatments implemented by lawyers as part of the exercise of their profession on an individual basis.	No
Treatments implemented by the clerks of the commercial courts for the exercise of their activity.	No
Treatments implemented by notaries for the exercise of their notarial activity and drafting of documents of notary offices.	No
Treatments implemented by local authorities and legal persons under public and private law for the purpose of managing services relating to school, extracurricular and early childhood affairs.	No
Processing implemented for the sole purpose of managing physical access controls and schedules for the calculation of working time, outside of any biometric device. Excluding data processing which reveals sensitive or highly personal data.	No

[7] The approach taken by CNPD indicates those activities which are expressly exempt from the obligation to carry out a DPIA and generally conforms with EDPB guidelines with regards to those that should perform one.

Treatments relating to breathalyzers, strictly framed by a text, and implemented within the framework of transport activities for the sole purpose of preventing drivers from driving a vehicle under the influence of alcohol or drugs.	No

None of the envisioned PLATOON activities is either exempt from DPIA requirement nor are they likely to result in a high risk to the rights and freedoms of natural persons based on the criteria set by the French DPA and the EDPB.

Italy

- Personal Data Protection Code
- List of processing operations requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679

Activities requiring data protection impact assessments (Italy)	**Taking place in PLATOON?**
1. Large-scale evaluation or scoring treatments, as well as treatments involving the profiling of data subjects as well as carrying out predictive activities also carried out online or through apps, relating to "aspects concerning professional performance, economic situation, health, preferences or personal interests, reliability or behavior, location or movements of the interested party ".	No
2. Automated treatments aimed at making decisions that produce "legal effects" or that affect "in a similar way significantly" on the interested party, including decisions that prevent you from exercising a right or to use a good or service or to continue to be part of an existing contract (e.g. screening of customers of a bank through the use of data recorded in a risk center).	No
3. Treatments which provide for the systematic use of data for the observation, monitoring or control of the interested parties, including the collection of data through networks, also made online or through apps, as well as the treatment of unique identifiers capable of identifying users of the company's services of information including web services, interactive TV, etc. with respect to usage habits and vision data for prolonged periods. This also includes metadata treatments e.g. in telecommunications, banks, etc. carried out not only for profiling, but more generally for organizational reasons, of budget forecast, technological upgrade, network improvement, offer of anti-fraud, anti-spam, security services etc.	No
4. Large-scale processing of extremely personal data (see WP 248, rev. 01): reference is made, among others, to the connected data to family or private life (such as data relating to electronic communications whose confidentiality must be protected), or which affect the exercise of a fundamental right (such as location data, whose collection jeopardizes the freedom of movement) or whose violation entails a serious impact on the daily life of the data subject (such as the financial data that could be used to commit fraud relating to payments).	No
5. Treatments carried out in the context of the employment relationship using technological systems (also with regard to video surveillance and geolocation systems) from which derives the possibility of carrying out a remote control of employee activity (see the provisions of WP 248, rev. 01, in relation to the criteria nn. 3, 7 and 8).	No

6. Non-occasional processing of data relating to vulnerable subjects (minors, disabled, elderly, mentally ill, patients, asylum seekers).	No
7. Treatments carried out through the use of innovative technologies, also with particular organizational measures (e.g. IoT; artificial intelligence systems; use of online voice assistants through voice and textual scanning; monitoring carried out by wearable devices; proximity tracking such as wi-fi tracking) whenever at least one of the criteria identified in the WP also occurs 248, rev. 01.	Maybe (aggregated occupancy readings are taken in some pilots)
8. Treatments involving the exchange between different large-scale data holders with telematic methods.	No
9. Processing of personal data carried out through the interconnection, combination, or comparison of information, including the treatments that involve the crossing of consumption data of digital goods with payment data (e.g. mobile payment).	No
10. Treatments of categories of data pursuant to art. 9 or data relating to criminal convictions and offenses referred to in art. 10 interconnected with other data personal collected for different purposes.	No
11. Systematic processing of biometric data, considering the volume of data, duration, or persistence, of the processing activity.	No
12. Systematic processing of genetic data, considering the volume of data, duration, or persistence, of the processing activity.	No

None of the envisioned PLATOON activities is likely to result in a high risk to the rights and freedoms of natural persons based on the criteria set by the Italian DPA.

Serbia

- Law on Personal Data Protection "Official Gazette of RS" no. 87/2018 of 13.11.2018
- Law on ratification of the Convention for the protection of persons with respect to the automatic processing of personal data
- List of processing activities requiring a data protection impact assessment (DPIA)

Activities requiring data protection impact assessments (Serbia)	Taking place in PLATOON?
1) systematic and comprehensive assessment of the condition and characteristics of a natural person performed by automated processing of personal data, including profiling, on the basis of which decisions are made relevant to the legal position of an individual or similarly significantly affect him;	No
2) processing of special types of personal data, i.e. data revealing racial or ethnic origin, political opinion, religious or philosophical belief or trade union membership, as well as processing of genetic data, biometric data for the purpose of unique identification of persons, health data or data on the sexual life or sexual orientation of a natural person or personal data related to criminal convictions and criminal offenses and security measures, to a large extent;	No
3) systematic supervision of publicly available areas to a large extent;	No
4) processing of personal data of children and minors for the purpose of profiling, automated decision-making or for marketing purposes;	No
5) use of new technologies or technological solutions for the processing of personal data or with the possibility of processing personal data that serve to analyze or predict the economic	Maybe (aggregated occupancy

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>situation, health, preferences or interests, reliability or behavior, location or movement of individuals;</td><td>readings are taken in some pilots)</td></tr>
<tr><td>6) processing of personal data in a manner that includes monitoring the location or behavior of the individual in the case of systematic processing of communication data generated by the use of telephone, internet or other means of communication;</td><td>No</td></tr>
<tr><td>7) processing of biometric data for the purpose of unique identification of employees by the employer and in other cases processing of personal data of employees by the employer using applications or systems for monitoring their work, movement, communication, etc.;</td><td>No</td></tr>
<tr><td>8) processing of personal data by crossing, linking, or checking matches from several sources;</td><td>No</td></tr>
<tr><td>9) processing of special types of personal data for the purpose of profiling or automated decision-making.</td><td>No</td></tr>
</table>
<b>None of the envisioned PLATOON activities is likely to result in a high risk to the rights and freedoms of natural persons based on the criteria set by the Serbian DPA.</b>
</td>
</tr>
<tr>
<td><b>Spain</b></td>
<td>
<ul>
<li>Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights</li>
<li>Law 34/2002, of July 11, on services of the Information Society and Electronic Commerce.</li>
<li>General Telecommunications Law 9/2014, of May 9.</li>
<li>List of processing operations not requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679</li>
</ul>
<table>
<tr><th>Activities exempt[8] from data protection impact assessments (Spain)</th><th>Taking place in PLATOON?</th></tr>
<tr><td>1. Processing carried out strictly under the guidelines established or authorized previously, by way of circulars or decisions issued by supervisory bodies, specially the AEPD, whenever the processing has not changed since it was authorized;</td><td>No</td></tr>
<tr><td>2. Processing carried out strictly under the guidelines of codes of conduct approved by the Commission or by supervisory bodies, specially the AEPD, whenever a full DPIA has already been carried out within a context of a validated code of conduct, and is implemented with the measures and safeguards defined in the DPIA;</td><td>No</td></tr>
<tr><td>3. Processing that is necessary in order to comply with a legal requirement or to complete a mission being carried out in the public interest or in the exercise of official authority vested in the controller, provided that there is no duty to carry out a DPIA within the legal mandate itself, whenever a full DPIA has already been performed;</td><td>No</td></tr>
<tr><td>Processing carried out by self-employed personnel who work on an individual basis in the exercise of their professional duties, specially physicians, healthcare professionals, or lawyers, notwithstanding that it may be required when the processing</td><td>No</td></tr>
</table>
</td>
</tr>
</table>

[8] The approach taken by AEPD indicates those activities which are expressly exempt from the obligation to carry out a DPIA and generally conforms with EDPB guidelines with regards to those that should perform one.

	carried out complies, in a significant way, with two or more criteria established in the list of types of data processing that require impact evaluation relative to data protection published by the AEPD;	
	5. Processing carried out in relation to the internal administration of personnel working at SMEs, in order to face processing operations mandatory by law for the purposes of accounting, human resources management, payroll management, social security, and safety in the workplace, but never in relation to customer data;	No
	6. Processing carried out by owners' associations and sub-associations in multioccupancy properties, according as these are defined at article 2 (a, b, and d) of Law 49/1960 on Horizontal Property;	No
	7. Processing carried out by professional colleges and non-profit associations in connection with the data of their associates members and donors of the data controllers listed therein concerning the management of their personal data, and in the performance of their tasks, provided that the processing does not extend to sensitive data such as those referred to in article 9.1 of the GDPR and that article 9.2(d) does not apply;	No
	None of the envisioned PLATOON activities is either exempt from DPIA requirement nor are they likely to result in a high risk to the rights and freedoms of natural persons based on the criteria set by the Spanish DPA and the EDPB.	

Table 2 Relevant National Laws and DPIA Criteria

2.3 Ethics framework

As a H2020 project, PLATOON recognizes the integral role that ethical[9] considerations take throughout the project's lifecycle. Its partners are committed towards the demonstration of ethical compliance as a pivot to achieve real research excellence. Ethical research conduct implies the application of fundamental ethical principles and legislation to scientific research in all possible domains of research. All partners have committed to respect the following principles throughout the research activities carried out by the project and to introduce specific measures to support these principles in the enablers and solutions to be developed by the project:

- Human dignity
- Freedom
- Democracy, citizenship, and participation
- Privacy
- Autonomy and informed consent
- Justice
- Solidarity

Furthermore, PLATOON partners have expressly agreed to comply with the H2020 ethics guidelines and have manifested their commitment to the principles of the European Convention of Human Rights.

[9] "Information ethics has been defined as "the branch of ethics that focuses on the relationship between the creation, organization, dissemination, and use of information, and the ethical standards and moral codes governing human conduct in society". (Joan, 2010)

Any arising ethics-related issues generated from this project will be handled in direct accordance with the principles noted in the following ethical frameworks:

- Helsinki Declaration of 1964 (revised version 2004)
- European Convention of Human Rights
- Rules of the Convention of the Council of Europe for the protection of individuals (automatic processing of personal data)
- Charter of fundamental human rights (Art. 8, 2000)
- General Data Protection Regulation 2016/679

Ethical responsibilities for PLATOON partners

As described in the PLATOON DoA, partner responsibilities related to ethical issues have been agreed upon, and the following guidelines shall apply in relation to compliance, approvals, privacy, personal health information and collaboration within the project:

- Each party represents that it has all necessary third-party consents to permit distribution and use of the data and any other information provided to other parties.
- Any party which provides any data or information to another party in connection to the project will not include any personal information relating to an identified or identifiable natural person or data subject.
    - To this end, the providing party will anonymize all data delivered to other parties to an extent sufficient to ensure that a person without prior knowledge of the original data and its collection cannot, from the anonymized data and any other available information, deduce the personal identity of subjects.
    - Each party shall be solely responsible for the selection of specific database vendors/data collectors/data providers, and for the performance (including any breach) of its contracts between it and such database vendors/data collectors, (to which no other project partner shall be a party, and under which no other partner assumes any obligation or liability), and shall further warrant that it has the authority to disclose the information, if any, which it provides to the other parties, and that where legally required and relevant, it has obtained appropriate informed consents from all the individuals involved.
    - Partners supplying special data analysis tooling shall have the right on written notice and without liability to terminate the license that it has granted for such tooling to be used in connection with the project, if the supplying partner knows or has reasonable cause to believe that the processing of particular data through such tooling infringes the rights (including without limitation privacy, publicity, reputation and intellectual property rights) of any third party, including of any individual.

PLATOON will follow an Ethical design process whereby all partners will seek to ensure their solutions and enablers

a) generate trust in the data subjects and end-users;
b) addresses the digital divide and introduces simple interfaces which consider the needs of the diverse end-users;
c) ensures transparency and accountability, both in the information provided through the diverse graphical elements of the platforms, and the information to be kept to demonstrate compliance;
d) prevents unpredictable behavior (through the introduction of logical safeguards to prevent any affectation to the rights and freedoms of all involved partners);
e) prevent functionality obfuscation and seek informed consent.

Ethical Committee and DPO network

Mandat International, specialized in ethics issues, has been appointed to constantly monitor and adequately address the ethics and social issues connected with the PLATOON project, including ethics evaluation of the Bottom-up Projects selected for the experiments[10]. PLATOON will take care that the projects selected through Open Calls apply to the ethical standards and guidelines of Horizon 2020 by establishing an Ethics Committee (Section 3.2.1) which includes independent expertise to supervise and monitor the ethical concerns in the project. This action will be implemented in close alignment with the H2020 Ethics Appraisal Procedure[11].

The Ethical Committee will review all projects selected, subject them to strict ethical screening/requirements on personal data protection and any other potential ethical issues. If any project seems to have Ethical issues the Committee will indicate the specific actions to be taken (contractual requirements wherever necessary) and will participate in the monitoring sessions of these projects during the entire project life cycle.

At the time of preparation of this Deliverable, no Ethics related concerns have been identified in the PLATOON Project, its enablers, solutions or expected activities. The Ethical Committee will closely follow the developments to be carried out throughout the project and will coordinate with Tasks 3.5 and 10.4 to introduce any required updates to the requirements specified throughout this document.

[10] As described in the PLATOON DOA for Task 7.3: “Once the selection has been done, Third Parties Legal & Financial Validation will take place [FBA]: The Provisional FSTP Sub-grantees have to provide all documentation required to prove their compliance with the Eligibility Criteria and for the Legal and Financial Check. Ethics Review. All main listed proposals are verified by the ‘Ethical Committee’ (In charge of verifying that there are no ethics issues in the selected proposals. It will be composed by Ethics Experts from PLATOON partners and be coordinated by MI.) to see if there are any ethics issues raised in the proposal. If so, an ‘Ethics Summary Report’ will be produced.

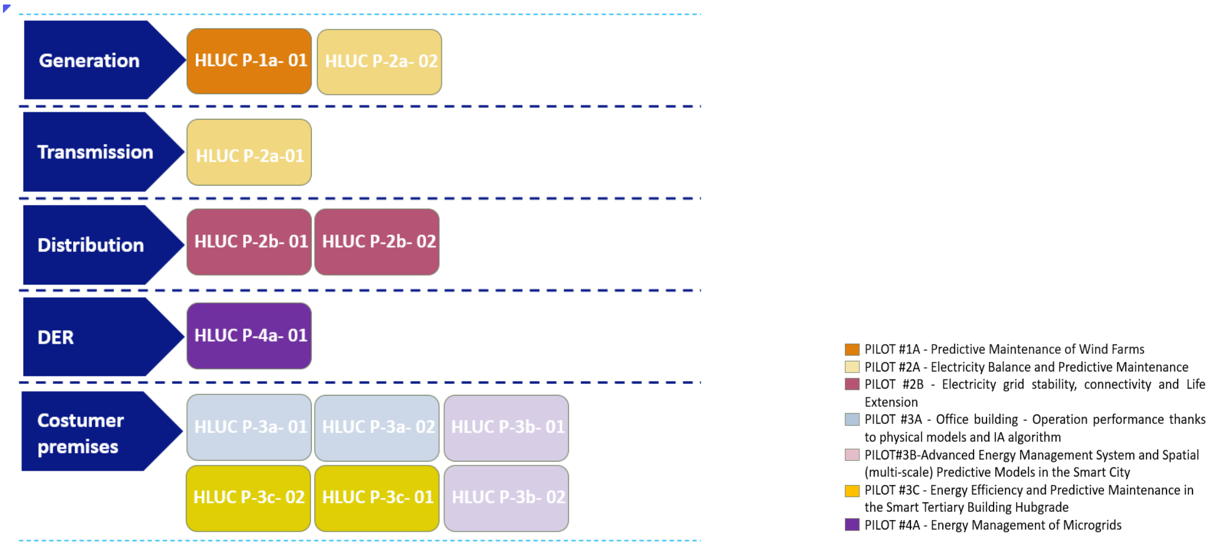
[11] As noted in https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm. FSTP recipients will be required to fill in an ethics issues table in close alignment with the H2020 model (example available at: https://ec.europa.eu/research/participants/portal/doc/call/h2020/msca-rise-2014/1597696-ethics_issues_table__checklist_en.pdf)

3 Component overview and Personal Data Protection Assessment

This section introduces a high-level overview of the PLATOON Pilots, Open Calls and Solutions to be developed, and performs a Personal Data Protection Assessment (based on the information available thus far) which will serve as a baseline for the work to be performed by Task 3.5.

3.1 PLATOON Pilots

This section presents a brief overview of the Pilots and associated High-Level Use-Cases (HLUC) and Low-Level Use-Cases (LLUC) as defined in PLATOON D.1.1. The Hight Level Use Cases describe business functions, i.e., the business layer of the SGAM framework. The functional description of the LLUCs identifies the services and tools required to perform a specific step of the main function.
The following figures depict the HLUC and LLUC divided into the five SGAM business domains.


Generation
HLUC P-1a- 01
HLUC P-2a- 02
Transmission
HLUC P-2a-01
Distribution
HLUC P-2b- 01
HLUC P-2b- 02
DER
HLUC P-4a- 01
Costumer premises
HLUC P-3a- 01
HLUC P-3a- 02
HLUC P-3b- 01
HLUC P-3c- 02
HLUC P-3c- 01
HLUC P-3b- 02
PILOT #1A - Predictive Maintenance of Wind Farms
PILOT #2A - Electricity Balance and Predictive Maintenance
PILOT #2B - Electricity grid stability, connectivity and Life Extension
PILOT #3A - Office building - Operation performance thanks to physical models and IA algorithm
PILOT#3B-Advanced Energy Management System and Spatial (multi-scale) Predictive Models in the Smart City
PILOT #3C - Energy Efficiency and Predictive Maintenance in the Smart Tertiary Building Hubgrade
PILOT #4A - Energy Management of Microgrids

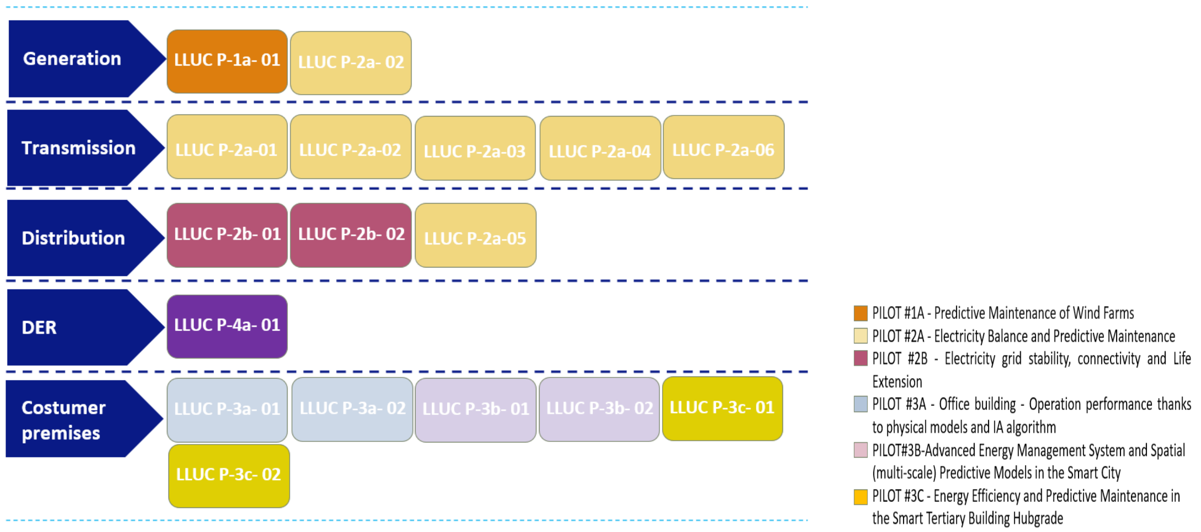

Generation
LLUC P-1a- 01
LLUC P-2a- 02
Transmission
LLUC P-2a-01
LLUC P-2a-02
LLUC P-2a-03
LLUC P-2a-04
LLUC P-2a-06
Distribution
LLUC P-2b- 01
LLUC P-2b- 02
LLUC P-2a-05
DER
LLUC P-4a- 01
Costumer premises
LLUC P-3a- 01
LLUC P-3a- 02
LLUC P-3b- 01
LLUC P-3b- 02
LLUC P-3c- 01
LLUC P-3c- 02
PILOT #1A - Predictive Maintenance of Wind Farms
PILOT #2A - Electricity Balance and Predictive Maintenance
PILOT #2B - Electricity grid stability, connectivity and Life Extension
PILOT #3A - Office building - Operation performance thanks to physical models and IA algorithm
PILOT#3B-Advanced Energy Management System and Spatial (multi-scale) Predictive Models in the Smart City
PILOT #3C - Energy Efficiency and Predictive Maintenance in the Smart Tertiary Building Hubgrade
PILOT #4A - Energy Management of Microgrids

Figure 1 PLATOON's LLUC classification according to SGAM – domains

For each Pilot, a short description is provided alongside a description of the data sources to be used, the potential for compilation or generation of personal data, and the specific actions or methods undertaken by the pilot owner to prevent use/misuse of personal data. These are followed with a High-Level PDP overview of the use-cases, for which a short description of each HLUC is presented alongside a brief characterization of its main processing activities. Finally, each LLUC generated from the HLUC are identified, described and accompanied with a table specifying whether personal data will be involved, whether technical and organizational measures are in place to protect personal data, and whether risks to the rights and freedoms to the data subjects could be envisioned at this stage of the project. This assessment will serve as a baseline for future PDP related activities in the project.

3.1.1 PILOT #1A - Predictive Maintenance of Wind Farms

The goal of this pilot is the development of an integrated monitoring strategy for predictive maintenance of electrical drivetrain components, more specifically the generator and the power converter of wind turbines. Focus is on the combination of data-driven models with physical models of the generator and potentially of the power converter into an integrated digital twin strategy. High frequency (kHz range) detailed measurements will be used in a first step. In a later stage, the focus of the analysis will shift towards fleet-wide analytics. At this stage lower frequency SCADA data (10-min) and status logs are used. In addition to the anomaly detection for problem identification also load history of the electrical components is identified. The potential for edge computations of the models is explored. More specifically, the optimization of the computational load for anomaly detection is investigated.

Data sources to be used:

The data that will be used in this pilot is wind turbine sensor data. The first subset of data is coming from dedicatedly performed high-frequency measurements using sensors mounted on the electrical subcomponents of the wind turbine (generator and converter). A second subset originates from controller data (SCADA data) consisting of 10-minute averages of sensor readings and status logs. In addition, external parameters (e.g. humidity) are used.

Potential for personal data to be compiled in the context of the trial and/or generated by the pilot:

None. Only machine data is used.

Specific actions/methods undertaken by the pilot owner to prevent use/misuse of personal data:

All data except open data is shared under NDA.

High-level PDP Overview of Use Cases:

A) HLUC-P-1a- 01: Predictive Maintenance for Wind Improve Wind Turbine Uptime with X%

Short description

The main goal of this pilot is to reduce operations and maintenance costs linked to unexpected downtimes for a fleet of wind turbines.

This HLUC is related to the development of an integrated monitoring strategy for predictive maintenance of electrical drivetrain components, more specifically the generator and the power converter of wind turbines. Focus is on the combination of data-driven models with physical models of the generator and potentially of the power converter into an integrated digital twin strategy. High frequency (kHz range) detailed measurements will be used in a first step. In a later stage, the focus of the analysis will shift towards fleet-wide analytics. At this stage lower frequency SCADA data (10-min) and status logs are used. In addition to the anomaly detection for problem identification also load history of the electrical components is identified. The potential for edge computations of the models is explored. More specifically, the optimization of the computational load for anomaly detection is investigated.

It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Study of how the failure mode works
- Modelling process to capture failure mode influence factors
- Validate model with known failure cases -> Confusion Matrix
- Increase robustness software code

LLUC generated from this Use case:

- ***LLUC P-1a- 01: Enhanced diagnostics of failure in electrical drivetrain components in wind turbines using a digital twin approach:*** development of an integrated monitoring strategy for predictive maintenance of electrical drivetrain components. Focus is on the combination of data-driven models with physical models of the generator and potentially of the power converter into an integrated digital twin strategy.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 3 Initial PDP Assessment for LLUC P-1a-01

3.1.2 PILOT #2A - Electricity Balance and Predictive Maintenance

In coordination with the European Network of Transmission System Operators (ENTSO-E) and the Energy Community (an international organization established between the European Union and a number of third countries to extend the EU internal energy market to Southeast Europe), the balancing market with the exchange of reserves is developed in the West Balkan region and Southeast Europe. The exchange of a primary reserve between two TSOs is most developed one, while the process of activating secondary and tertiary reserves in order to maintain the sum of power exchange with the neighboring power systems and frequency at the planned value is part of the balancing (of power system) activities. At the end of 2007, Serbian TSO (System operator) has taken over the coordination of joint billing and control block of Electric Power Industries of Serbia, Montenegro and North-Macedonia (ENTSO-E SMM control block). Currently, the Electric Power Industry of Serbia (PE EPS) is the only supplier of the balance reserve, but independent producers (IPP) and producers from distributed and renewable sources (DER) will be actors in the balance reserve market in the future.

Hence the PLATOON Pilot #2a Electricity Balance and Predictive Maintenance that is taking place in Serbia has been elaborated taking in mind the need for analytical services that could improve the electricity balance and predictive maintenance. Several use cases have been developed that are categorized according to priority into High (services needed and will be developed), Medium (nice to have), Low (out of scope or too specific to the Pilot).

Data sources to be used:

Data sources in the above scenarios are

- the IMP proprietary SCADA system
- the CS phasor measurement unit (PMU) that will be used together with IMP SCADA

Potential for personal data to be compiled in the context of the trial and/or generated by the pilot:

No personal data will be needed for implementation / testing of the scenarios.

Specific actions/methods undertaken by the pilot owner to prevent use/misuse of personal data:

As no personal data will be needed for implementation / testing the scenarios, no specific actions are necessary.

High-level PDP Overview of Use Cases:

A) HLUC P-2a- 01: Electricity Balance

Short description

In this use case, PLATOON services will be developed that will upgrade the IMP SCADA system with electricity balancing functionalities needed in case of power injections from wind farms. With the increased penetration of distributed generation (e.g. wind power), the risk of temporary imbalances also increases caused by wind power uncertainties due to its dependence on the volatility of the wind. So, advanced demand/response optimization services are needed to prevent power outages or blackout (complete interruption of power in each service area). The role of the SCADA / EMS on the production side is monitoring and control of generation and data exchange.

It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Study of supply and demand variables
- Integration of the state estimation (SE) applications with the IMP proprietary SCADA system
- ML models based on historical data to address the balancing challenges for the system operator due to increasing amounts of renewable energy sources embedded within the distribution networks (e.g. solar photovoltaic (PV), wind power plants)
- Integration with the state estimation applications
- Testing and validation

LLUC generated from this Use case

- **LLUC P-2a-01 Balancing on regional level:** Dedicated to explaining the electricity balancing process on regional level, focused on generating cost-efficient distribution and transmission, increasing annual net savings from tertiary reserve trading, responding better to changes in demand and avoiding curtailment.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 4 Initial PDP Assessment for LLUC P-2a-01

- **LLUC P-2a-02 Balancing on country level:** concentrates on tertiary reserve/energy exchange process, particularly towards ensuring cost-efficient distribution and transmission, better demand response, improved res integration and balancing of the energy portfolio of Balance Responsible Parties (in the Serbian electricity market, all market participants are balancing parties and their relations are regulated by contracts). Particularly towards ensuring cost-efficient distribution and transmission, better demand response, improved res integration and balancing of the energy mix.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 5 Initial PDP Assessment for LLUC P-2a-02

- **LLUC P-2a-03 Demand forecast on transmission level:** Which describes the use of PLATOON tools for load demand forecast analysis. Load demand forecasting involves the accurate prediction of both magnitudes and geographical locations of the electric load over the different periods of the planning horizon. This LLUC focuses on ensuring cost-efficient distribution and transmission and better demand response.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 6 Initial PDP Assessment for LLUC P-2a-03

- **LLUC P-2a-04 RES (Wind generation) forecasters:** Which aims to develop and test a PLATOON service for more accurate prediction of renewable energy generation, focusing particularly on curtailment avoidance, portfolio optimization and cost-efficient distribution and transmission.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 7 Initial PDP Assessment for LLUC P-2a-04

- **LLUC P-2a-05 Effects of Renewable Energy Sources on the Power System (distribution level):** Focused on testing the PLATOON analytical services for analysis of unexpected variations (voltage profile of the power system) before and after RES integration to the power system. This LLUC will particularly seek to Improve RES integration, balance energy mix, avoid curtailment and increase stability.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 8 Initial PDP Assessment for LLUC P-2a-05

- **LLUC P-2a-06 Research Data Management:** This LLUC showcases how the process of storing and retrieval of artefacts (data models, external datasets, research results/outputs) can be managed with a CKAN repository. It will generate a tool to this end, focused on the generation of metadata models, running statistical algorithms, and support of visualizations.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 9 Initial PDP Assessment for LLUC P-2a-06

B) HLUC P-2a- 02: Predictive Maintenance in RES power plants

Short description

This HLUC seeks to develop a predictive layer on top of exiting SCADA at a thermal power plant.
It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Integration of SCADA with PLATOON tools
- ML model based on historical data given the system's parameters, to draw strategies to deal with similar events in the future
- ML model for real-time monitoring of advanced sensors and monitoring equipment
- Communication with emergency services
- Testing and validation of the service (SCADA for Thermal Power Plant)

LLUC generated from this Use case

- **LLUC P-2a- 07 Predictive maintenance in RES power plants:** Envisioned activities seek to design, develop and test a set of machine learning algorithms to perform predictive maintenance of power plant infrastructure, focusing particularly on ensuring increased stability and reducing maintenance costs.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 10 Initial PDP Assessment for LLUC P-2a-07

3.1.3 PILOT #2B - Electricity grid stability, connectivity and Life Extension

This pilot is focused on reinforcing reliable operation of the power grid using advance tools in energy management, controls systems, power grid operation and planning tools.

To this date, two different Use Cases have been defined, one focused on the development of a predictive maintenance tool for LV/MV transformers using available data from Sampol´s smart grid in ParcBit, Majorca (Spain) and define a transformer maintenance plan; and a second one aimed to develop a tool for the quantification of losses in the distribution grid of a DSO and the detection of non-technical losses (NTL), using the available smart meter data from Sampol´s smart grid in ParcBit, Majorca (Spain).

Data sources to be used:

The Mallorca pilot is based on monitoring some transformers and visualize their maintenance while their aging. Different sensors will be installed to monitor transformer physical data such as top oils temperature, oil pressure, oil level, external temperature. Also, electrical data will be collected from the primary and the secondary circuits of the transformer.

To have a clear picture of the energy balance of the Parc Bit grid, Smart Meter registers of corporate consumers (prosumers) will be processed.

Potential for personal data to be compiled in the context of the trial and/or generated by the pilot:

Parc BIT is a technological parc composed by companies, only aggregated datasets (per company) will be utilized and no personally identifiable data will be utilized or generated. There is not personal data compiled or generated in this pilot.

Specific actions/methods undertaken by the pilot owner to prevent use/misuse of personal data:

No specific actions are required given the lack of personal data in this pilot. As detailed below, preventative measures (privacy by design approach) is being set in place to minimize potential issues of NTL detection component during post-PLATOON exploitation.

High-level PDP Overview of Use Cases:

A) HLUC P-2b- 01: Predictive Maintenance in Transformers

Short description

This HLUC focuses on transformer predictive maintenance, estimating transformer components health and its maintenance costs, planning maintenance actions, monitoring transformer alarms, and studying different grid scenarios in case of replacing old transformers or adding complementary transformers.

It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Compile available technical transformer information and measurements, and maintenance logs, and create a database for the asset health management platform
- Exploratory data analysis, including data cleaning and pre-processing, and labialization of the dataset: Identification of faulty periods and check the maintenance logs
- Calculate the RUL of the critical components of the transformer, for different failure modes, due to aging in working conditions
- Calculate the health index of the transformer
- Economic calculation to define the optimal maintenance plan of the transformer
- Model to simulate the effect of different operational actions in the grid O&M cost sheet.
- Implement and validate the asset health management platform

LLUC generated from this Use case

- **LLUC P-2b- 01 Predictive Maintenance for MV/LV Transformers:** Which focuses on transformer predictive maintenance, estimating transformer components health and its maintenance costs, planning maintenance actions, monitoring transformer alarms and studying different grid scenarios in case of replacing old transformers or adding complementary transformers. It particularly seeks to decrease risks, generate savings (including the reduction of maintenance costs), and extend the useful life of transformers.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 11 Initial PDP Assessment for LLUC P-2b-01

B) HLUC P-2b- 02: Non-technical loss detection

Short description

This HLUC considers different techniques to calculate the losses, detect NTL appearance and identify NTL authors (prosumers and non-customers) using data from the smart meters of prosumers and measurements at the substations and transformation centres-CTs.

It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Gather electricity grid topology and parameters.
- Gather historical load data, at the MV substation level, and for the smart meter of each of the prosumers connected to the distribution grid.

- Historical load data cleaning and pre-processing.
- Labialization of prosumer load dataset: Identify historic known NTL, if any, based on evidence of fraud.
- Exploratory assessment of energy losses, based on energy balances, to determine thresholds of a reasonable level of technical losses.
- Prosumer segmentation based on clustering techniques applied to their load profiles.
- Development of an NTL detection algorithm to detect PTUs in which NTL would have occurred, based on losses higher than reasonable technical losses, which accuracy can be improved considering grid topology.
- Development of an NTL identification algorithm for identification of NTL authors, based on the detection of abnormal behaviours of prosumers. Development of this algorithm will involve coordination with both Sampol's DPO and PLATOON project DPO.
- Development of a software platform which integrates load data acquisition with use case logic (prosumer segmentation, NTL detection and identification algorithms), with a friendly user interface.
- Validation of NTL detection and identification algorithms.

LLUC generated from this Use case

- **LLUC- P-2b-02: Non-technical loss detection in Smart Grids:** This LLUC aims to develop a tool for the quantification of losses in the distribution grid of a DSO and the detection of non-technical losses[12] (NTL), using the available smart meter data from Sampol´s smart grid in ParcBit, Majorca (Spain). The envisioned solution will require only measurement data available from the Automatic Metering Infrastructure-AMI, and optionally information on the grid topology (no personally identifiable information necessary). This use-case will particularly seek to identify percentages of non-technical losses and increase savings due to detected losses.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
During PLATOON Pilot: **None**: Company-level data will be used.	**In place:** Anonymization (Aggregation), Data minimization.	**Negligible**, the location of the trial and the aggregated nature of the datasets from smart meters in place, along with the corporate nature of the consumers prevents risks from arising directly from the project.
Post-project (exploitation): **Potentially** (Outside Project-scope)	**In place:** Privacy by Design, Data minimization.	**Moderate** (depending on the implementation of the solution in a production environment (outside the scope of the PLATOON project), NTL identification solutions could lead to the identification of individuals).

Table 12 Initial PDP Assessment for LLUC P-2b-01

[12] Non-technical losses (NTL) in the electric system is one of the biggest fraud factors, generally due to smart meter and/or connection to the grid (bypass of certain consumer loads) manipulation. NTL can be attributed to i) administrative losses due to accounting errors and record keeping, ii) customer theft, iii) customer non-payment and iv) theft by non-customers.

3.1.4 PILOT #3A - Office building - Operation performance thanks to physical models and IA algorithm

The pilot 3a concerns an office building with a focus on developing Use Cases to optimize the HVAC system performance or provide new kind of services (to help with the grid management).

Data sources to be used:

The list of the data collected or calculated to realize the services described in the use cases are presented in the table below:

Data	Categories	Recipients	Persons with access to the data
Recorded data from BMS: • Internal air temperature in building • Temperature setpoints • Valve controls for heating and cooling • Consumption data of HVAC system (heating and cooling in the building) **Recorded data from external data provider:** • Weather data (temperature and solar radiation) • Weather data forecast **Recorded data from occupancy sensors:** • Occupancy data in the different zones of the building *NB: the exact technology and type of sensors has not been defined yet*	Common data relative to building but no personal data. Data (potentially sensitive): aggregated occupancy data in the building (but not linked to a user)	PLATOON platform	Authorized staff at ENGIE
Calculated data: • Occupancy prediction in the different zones of the building. • Time for preheating/precooling in the building (to optimize controls) • Prediction of the HVAC load and prediction of the load flexibility	Data: aggregated occupancy predictions in the building (but not linked to a user)	PLATOON platform	Authorized staff at ENGIE

Table 13 Data Management and classification in pilot 3a

Potential for personal data to be compiled in the context of the trial and/or generated by the pilot:

The only data that could lead to the generation of personal information is the occupancy data collected in the building. The occupancy data used will be aggregated (no individual tracking is possible and no correlation with personnel-related databases possible) by zones. As specified previously, the technology and type of occupancy sensor that will be used are not defined yet, however, preference will be given to solutions that respect personal data protection principles, including the following:

- Occupancy data manipulated in the project will not be associated with a given individual: only aggregated data for the different zones of the building will be stored and processed (no more details are required).

- Each floor will be subdivided into 2-4 zones and each zone will cover a space that cannot be associated with a specific individual (it could be only associated to a team or a given group of people).

Specific actions/methods undertaken by the pilot owner to prevent use/misuse of personal data:

No personally identifiable information is expected to be collected or manipulated in the scope of the pilot. Specific technical and organizational precautions will be given vis-à-vis the occupancy data that will be collected in the project, to confirm that the technology and the type of sensor will not produce data that could be associated (precisely or partially) to a specific person.

High-level PDP Overview of Use Cases:

A) HLUC-P-3a- 01: Save X% on the GHG emissions

Short description

This HLUC concerns the reduction of energy consumption and greenhouse gases emissions for the building. It can be realized through optimization of HVAC operation and controls in the building, as well as the use of local renewable energy sources (PV) that could be installed on the building. The different possibilities and strategies to reduce the energy consumption, using the data available on the building and the different equipment, will be evaluated and tested.
It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Compile and clean data available for the building for a full year (focused on high-level technical-focused and aggregated building datasets)
- Implement an algorithm to compare yearly data (occupancy, climate, energy efficiency of appliances, etc.)
- Digital twin of the building compatible with energy management constraints and test management strategies

LLUC generated from this Use case

- **LLUC P-3a-01 Optimization of HVAC operation regarding building occupancy:** This use-case intends to provide a smart module for an office building that optimize HVAC operation in the function of real occupancy. Occupancy data are available via dedicated sensors, and the comfort and HVAC controls are available via the Building Management System (BMS) of the building. Using historical data, some learning algorithm is implemented to predict occupancy and anticipate heating and cooling period in the building and its different zones. A first optimization loop can be implemented to control the overall building occupancy planning and HVAC operation. A second optimization loop is used to adapt HVAC controls in the different zones of the building. The building manager can supervise and update some parameters in the system and access some regular assessment of the system controls.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
Potentially (aggregated occupancy data)	**In place:** Anonymization (aggregation), Data Minimization	**Negligible** – The BMS will not provide personally-identifiable information and the deployed system won't collect or generate such data.

Table 14 Initial PDP Assessment for LLUC P-3a-01

B) HLUC-P-3a- 02: Power Management and flexibility

Short description

This HLUC concerns the electrical load management with flexibility services that could be offered to the grid. It can be realized through specifics controls of the electrical loads in the building: heating and cooling loads using the building inertia and other types of electrical load that could be shifted. Switching to other energy sources or using storage equipment (batteries, H2) could also be part of the scope. An analysis of the flexibility available in the building and the use of a digital twin can enable to evaluate the potential and predict the available flexibility on the building.

LLUC generated from this Use case

- **LLUC P-3a 02 Provide Demand Response services through building inertia and HVAC controls:** The use case intends to provide a smart module to supervise the implementation of Demand Response services in an office Building using HVAC control and building inertia. Collecting data on the building and using weather forecast, the module developed is providing predictions of the HVAC load and the potential flexibility available while maintaining a given level of comfort in the building.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None (only aggregated, historical datasets are used)	**Not Necessary**	**None**

Table 15 Initial PDP Assessment for LLUC P-3a-01

3.1.5 PILOT #3B - End Use of Energy - Advanced EMS (Energy Management System) and Spatial (multi-scale) Predictive Models

This pilot is divided between two main activities carried out by two partners, namely:

Poste Italiane:

Poste Italiane collects and manages big data related to energy use and consumption mainly from mid and big size buildings (spanning from 250 to 28.000 smq) but is also going to increase the depth and detail of data collected through progressive integration of existing energy consumption devices (lighting, heating, cooling technical plants, …) in a centralized database to be supported with Augmented Intelligence tools.

Poste Italiane participates in the Pilot #3b with a significative set of buildings in Rome in terms of dimension, destination, location and will send data consumption and other important information to the PLATOON Platform.

Rome Municipality:

Rome Municipality contributes to PILOT #3B with Use Case ROME-01, aiming to set up and deploy a Monitor and analysis system for the Data flow coming from 8950 energy meters of ROME Municipality buildings asset. The services that PLATOON will offer to energy manager office of ROM are spatial reporting, benchmarking analysis, forecast on consumptions, RES potentialities scenarios.

No transmission of personal data is expected to take place between Poste Italiane and Rome Municipality.

Data sources to be used:

Poste Italiane:

6500 power meters and 2450 gas meters produce a large dataset about energy consumptions that represents the main source of information to create an advanced EMS. This dataset is not capable of identifying individual data subjects, as all meters provide measurements only on the total building behavior (aggregated data), and no information about specific spaces or single users are neither collected nor processed. Other data concerning the buildings will be transmitted to perform this use case and among these data, those relating to the average presence or general functions of people in the single building will be always aggregated.

Rome Municipality:

The pilot will not process **Personal Data**, it will focus on technical data on energy consumption energy, buildings characteristics, plants information, etc.

Potential for personal data to be compiled in the context of the trial and/or generated by the pilot:

Poste Italiane:

No personal data will be compiled or generated by the pilot.

Rome Municipality:

No personal data will be compiled or generated by the pilot.

Specific actions/methods undertaken by the pilot owner to prevent use/misuse of personal data:

Poste Italiane:

Only Anonymized datasets will be utilized. All internal data management processes and communication activities within the Poste Italiane conform to the ISO 27001:2013 (Information security management systems) standard.

Rome Municipality:

All internal data management processes and communication activities within Rome Municipality will be supervised by the DTD Department that will assure that only Anonymized datasets are utilized.

High-level PDP Overview of Use Cases:

A) HLUC P-3b- 01: Building Energy Management System

Short description

Poste Italiane manages around 220 buildings in the area of Rome Municipality. In the context of this HLUC, 16 of the 220 building are selected as ‘test set’ grouped according to the end use and characteristics: Data center, Logistic Centers, Retail, Office Space. These buildings will be used for modelling, benchmarking, evaluating PLATOON components and algorithms and optimization actions in the following areas: Cooling and Heating Plants Consumptions Forecasting; Cooling and Heating Plants Predictive Maintenance; Lighting Consumption Estimation.” The following table showcases the main features of this pilot.

Processing purposes	Enable Energy Experts in making decisions to better address energy consumption strategies and optimize the plants (heating and cooling) maintenance.
Processing stakes	Implement tools based on algorithms and machine learning techniques for End user of Energy in keeping with the legal framework and personal data security.
Controller	Poste Italiane (Data Owner)
Processor(s)	Poste Italiane (data owner), all partners involved in the project for development and realization of the Analytical Tools

Table 16 Overall Pilot 3b description

As shown in the following tables, this Pilot does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Compilation of relevant (non-personally identifiable) datasets from significative buildings in a predefined frequency and volumes
- Perform data analysis based on predefined criteria

Processes	Detailed description of the process
Sent the data to the PLATOON Platform	An Event Hub collects information by sensors and other sources produce by plants and buildings. The data are sent to the PLATOON servers, via directly through internet (asynchronous process) with a periodical flow.
Enter the data for selection criteria	The Energy Expert (accesses to the Platform) selects parameters for a specific service and analysis
Analyze data	Data analysis algorithms and machine learning techniques are run on the PLATOON servers to produce a report based on the request (energy consumption benchmarking or forecast, data correlation, predictive analysis, etc.)
Analysis Response	The platform generates the response data based on previous dialogues and the interests detected
Store the data on the servers	The result of calculated data is stored on the PLATOON servers
Send Predictive Alert	Based on monitoring services, when an anomalous behaviour in plants (heating/cooling) is detected, an automatic alert is sent to the Energy Expert

Table 17 Process mapping in Pilot 3b

Data Types	Categories	Recipients	Persons with access to the data
Building Master Data: Identification code, address, destination use, sqm, occupancy profile, etc.	Non-personal data	PLATOON Platform	Authorized staff at Poste Italiane and PLATOON Developers
Building Plant: plant type, characteristics, etc.	Non-personal data	PLATOON Platform	Authorized staff at Poste Italiane and PLATOON Developers
Climate and weather data: internal temperature and humidity, external temperature	Non-personal data	PLATOON Platform	Authorized staff at Poste Italiane and PLATOON Developers

Data consumption: Id building, KW/h	Non-personal data	PLATOON Platform	Authorized staff at Poste Italiane and PLATOON Developers
Information on Plants Fault: data of fault, type, etc.	Non-personal data	PLATOON Platform	Authorized staff at Poste Italiane and PLATOON Developers
Calculated data (What data will the system generate based on the inputs): reporting with technical information, predictive alert	Non-personal data	PLATOON Platform	Authorized staff at Poste Italiane and PLATOON Developers

Table 18 Data Management and Categorization in Pilot 3b

LLUC generated from this Use case

- **LLUC P-3b 01 Buildings Heating & Cooling consumption Analysis and Forecast:** This use case aims to Benchmark and predicts the consumption of cooling and heating plants installed in the 16 pilot buildings in the municipality of Rome (for both summer and winter seasons), taking into account the following factors.
  i. The cooling (power) and heating (power & gas) systems installed at the Italian Post buildings currently managed and monitored in many different ways depending on hardware & SW installed locally, skills of the building managers, maintenance service companies and energy experts following the building.
  ii. The correlation with external weather conditions, building characteristics and past performances together with a benchmark with a similar building which represents an area of optimization for both cooling and heating systems.
  iii. Sensors, meters, and other hardware produce information that through processing with forecasting algorithms and machine learning techniques, could be used to predict plants consumption and for the energy efficiency benchmarking.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 19 Initial PDP Assessment for LLUC P-2b-01

- **LLUC P-3b 02 Predictive maintenance of cooling & heating plants:** optimizing the number of interventions, and the number of plant failures through condition monitoring techniques to track the performance of the equipment during normal operation and to identify any anomalies and resolve them before they give rise to failures without increasing planned maintenance.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 20 Initial PDP Assessment for LLUC P-2b-01

- **LLUC P-3b 03 Lighting Consumption Estimation & Benchmarking:** The weight of consumption due to lighting is estimated to be greater than 20% of the overall electrical consumption of buildings. The scope of this use case is a deeper understanding of the lighting optimization levers and correlation (hours of artificial lighting use, number of users, sqm, …) order to reduce lighting consumption.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None (Aggregated occupancy data used only if necessary)	**In place:** Anonymization (Aggregation), Data minimization.	**Negligible**

Table 21 Initial PDP Assessment for LLUC P-2b-01

B) HLUC P-3b- 02: Building Asset Energy Management System

Short description

This HLUC includes about 1600 buildings owned by ROME with different uses and different plants and devices, including 165 photovoltaics, located in Rome. The data collected from the meters (power and gas) and the available Energy Audits will be sent to the PLATOON platform for energy consumption analysis and forecast, for anomalies detection, for automated validation/updating of energy efficiency scenarios, for data integration and new EMS tools implementation.

It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Collection of datasets (energy meters, energy audits)
- Perform data analysis based on predefined criteria and outputs
- Test data treatment and outputs for a control set of buildings
- Implement the data flow toward PLATOON Platform
- Carry out Big Data analytics and to the outputs' progressive assessment

LLUC generated from this Use case

- **LLUC P-3b 04 Monitor and analysis system for the Data flow coming from 8950 power and gas energy meters of ROME Municipality buildings assets:** The energy manager office of Roma Capital, within the SIMU Department, manages more than 8950 energy meters (6500 electric meters and 2450 gas meters) related to almost 2000 buildings owned by the municipality. To help the office in this activity, considering the huge amount of data coming from the meters each month, a monitor system shall be implemented.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None (Aggregated data used only if necessary)	**In place:** Anonymization (Aggregation), Data minimization.	**Negligible**

Table 22 Initial PDP Assessment for LLUC P-2b-01

3.1.6 PILOT #3C - Energy Efficiency and Predictive Maintenance in the Smart Tertiary Building Hubgrade

Giroa manages the PLATOON project with the #3C Nanogune pilot building with the implementation of two use cases Advanced EMS in Smart Tertiary Building and Predictive Maintenance in Tertiary buildings. With the objectives of performing advanced management of energy generation, consumption and distribution in tertiary buildings and improving internal maintenance policies by introducing predictive maintenance algorithms.

This will be done by using the more than 80 energy meters installed in the building in addition to the data provided by the BMS and the meteorological prediction services and the additional sensors that will be installed during the project. With all this, through the developments made at PLATOON, energy management and predictive maintenance management reports will be made.

Data sources to be used:

Individual analysis for each case of use of the data or equipment that is going to be used showcased the following results:

a) Advanced EMS in Smart Tertiary Building; both thermal and electrical energy meters from different areas of the building will be used, as well as comfort parameters and equipment operation parameters, in particular, the data from the following installations will be used: Photovoltaic installation, Electrical consumption of the 1st floor Nano, Thermal consumption 1st floor Nano, Cooling machine, Boiler, AHU, Fan coils, Comfort parameters divided into several zones[13], namely:
   - Cantina
   - Corridor
   - Offices
   - Meeting room
   - Open office area 1
   - Open office area 2

b) Predictive Maintenance in Tertiary buildings; the data provided by the SCADA of the existing equipment in the Nanogune building will be used, as well as the energy meters of the following equipment: Coolers, Boilers, Pumps, AHU, Fan Coils, Heating ring, Cooling ring.

Potential for personal data to be compiled in the context of the trial and/or generated by the pilot:

No personal data will be compiled or generated by the pilot.

Specific actions/methods undertaken by the pilot owner to prevent use/misuse of personal data:

All internal data management processes will be supervised by the DTD Department and will ensure that all information refers to general areas and parameters of the building and never to the people using it.

High-level PDP Overview of Use Cases:

A) HLUC P-3C- 01: Advanced EMS in Smart Tertiary Building

Short description

This HLUC addresses the main functionalities and requirements related to the advanced EMS to be implemented within PLATOON. The foresaid EMS will optimize the local renewable energy resources (RES) and HVAC operation as a function of building and RES characteristics, building comfort constraints, ambient conditions and energy market price following a multi-objective pattern which targets to reduce the overall energy bill and maximize the usage of RES.

It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Data extraction (and potential aggregation of external data sources (weather, electricity market ...) to extract remaining parameters.
- Data Cleaning: analyze the quality of the data and correct inconsistencies/errors (missing values, outliers, inconsistent values...)

[13] Only aggregated data will be used to identify the confort parameters

- Exploratory data analysis: analyze the data using visual and statistical methods (unipara metric analysis, multiparametric analysis, correlation analysis...), Pattern recognition and benchmarking.
- Data driven or hybrid model of the building which simulates the thermal behavior of the building using historical off-line data.
- Build, train and validate the HVAC optimization algorithm using historical off-line data. Validate the developed algorithm with online data and modify the algorithm as necessary to get acceptable performance. And implement the developed algorithm in the production system.

LLUC generated from this Use case

- **LLUC P-3c-01 Advanced EMS for Tertiary Buildings:** The main objective of the functionality described in this LLUC is to enhance existing BMS systems with capabilities to optimize the energy usage maximizing the use of local RES in order to minimize the energy bill. Building cooling or heating demands can be anticipated by pre-cooling or pre-heating strategies implementation. The use case applies to tertiary buildings in which there is already a BMS implemented that enables seamless access to building usage data (HVAC, lighting, occupancy schedules). No personal data will be obtained from the BMS. On top of the BMS, the PLATOON project will implement analytical models based on machine learning techniques will predict the building thermal demands as well as the local energy production. Based on those predictions, optimization algorithms will be implemented.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**In place:** Data minimization. Privacy by Design.	**None**

Table 23 Initial PDP Assessment for LLUC P-3c-01

B) HLUC- P-3C- 02: Predictive Maintenance in Smart Tertiary Building

Short description

This use case describes the process of the development and the implementation of predictive maintenance tools for the thermal control assets of smart tertiary buildings (Boilers, Chillers, Air Handling Units (AHU), Split Systems, Fan coils, Extractors and Pumps). As well as, improving the maintenance policy increasing the availability and useful life of these assets and reducing the general maintenance costs.

It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Data extraction, cleaning, analysis (using visual and statistical methods) and labelling.
- Simulate the normal status of the systems through a data-driven or hybrid model, analyse deviations from faulty points, and training of algorithms.
- Implement the developed algorithm in the production system.

LLUC generated from this Use case

- **LLUC P-3c 02 Predictive Maintenance in Smart Tertiary Building Assets:** Which seeks to improve the maintenance policies in the tertiary buildings by implementing the predictive maintenance solutions generated in the previous use-case in specific building assets, increasing the availability, increasing the useful life of these assets and reducing the general maintenance costs.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 24 Initial PDP Assessment for LLUC P-3c-02

3.1.7 PILOT #4A - Energy Management of Microgrids

This pilot will focus on case applies to a micro-grid test-bench (the MG2lab in the Department of Energy, Politecnico di Milano): a cutting edge microgrid integrating different Distributed Energy Resources (DERs) like solar, combined heat and power, battery and hydrogen storage and serving both electric and thermal load to power lighting, heating, desalination, electrical vehicles and electrical bikes.

The goal of the pilot is to study data-driven energy management able to deal with the increased complexity of the energy systems and to assess the advantages of innovative strategies, including EMS with real-time processing and optimization for small-scale/renewable electricity generation; Generation and load forecast; Smart storage/generation; and V2G.

Data sources to be used:

MG2Lab micro-grid test-bench.

Potential for personal data to be compiled in the context of the trial and/or generated by the pilot:

None, all datasets to be used are generated in the test-bench and no personal data of any kind will be compiled.

Specific actions/methods undertaken by the pilot owner to prevent use/misuse of personal data:

None are necessary due to the lack of personal data in the pilot.

High-level PDP Overview of Use Cases:

A) HLUC-P-4A- 01: Energy Management of Microgrids

Short description

This HLUC applies to a microgrid test-bench, to provide an analysis facility for real-life scale research, simulation, and test purposes.

The aforementioned microgrid test-bench is dedicated to improving the availability of big data and big data management, providing an analysis facility for real-life scale research, simulation and test purposes, thus allowing to study new data-driven paradigms for energy management able to deal with the increased complexity of the energy systems and to assess the advantages of innovative strategies.

It does not foresee personal data processing activities, as the planned activities focus on the following processes:

- Gather data from different sources internal/external (weather condition/forecast)
- Develop a robust optimization model for optimal power flow
- Implement the production system with edge computing capability.
- Develop an interface and data monitoring software
- Define optimal predictive maintenance actions.

LLUC generated from this Use case

- **LLUC P-4A 01 Energy Management of Microgrids:** Which will seek to study data-driven energy management able to deal with increased complexity of the energy systems and to assess the advantages of innovative strategies: EMS with real-time processing and optimization for small-scale/renewable electricity generation, Generation and load forecast; Smart storage/generation; V2G.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
None	**Not Necessary**	**None**

Table 25 High Level PDP Assessment for LLUC P-2b-01

3.2 PLATOON Open Calls

The PLATOON project will run two open calls, with the first launching in January 2021 and the second launching in 2022. The Data Controller will be FundingBox, which will coordinate all open-call related actions for the project. These open calls will require the collection of standard personal data[14][15] through the FBOX platform controlled by FundingBox, including the applicant's name, email address, phone number, place of residence/nationality, professional experience, education, and other professional information.

Processing purposes	Facilitate the technology transfer into the market by a well-established tendering process through Open Calls. Select the most relevant bottom-up projects **(identification and authentication of project proposers).**

[14] In addition to these elements, data related to the business activity of the participants and their participation in the program will be compiled.
A large part of the data managed in the project will be data related to SMEs participating in the Open Calls which, are considered confidential, yet the PLATOON partners will determine in the Data Management Plan (D10.4) which of the data they generate will be made open and available to the public. The type of data collected will include specific information to evaluate the potential of the proposals submitted and the proper execution of the proposals selected. Such information includes measurements of the innovation potential and maturity of proposals, the team and the organisation proposers, the technology used and technology experience, the market orientation, the financial aspects, and the benefits expected. Generic information is being collected in textual or numeric format, while the data regarding value propositions will be collected in a multiple-choice format.
The Consortium ensures confidentiality of the data included in the Application forms. Applicants will be advised to mark their confidential information as such. Personnel not involved in the open call execution will not have access to the application forms. The complete data flow will be described in detail in the data management plan.

[15] Personal data will only be required to join the on-line Community and during the evaluation of the PLATOON platform. However, all participants will be made fully aware that their involvement requires the submission of an Informed Consent Form, prior to their participation. This will empower the individuals involved to make a voluntary informed decision about whether or not to participate in the research based on knowledge of the purpose, procedures and outcomes of the research. The respect of their rights, as mandated by the GDPR will be guaranteed. Information on how the data will be managed will be provided in advance (Protection of Personal Data). MI will supervise all the procedures of data management. Personal data will also be processed in order to conclude the Agreement with third parties and run the acceleration program/pilot. Legal basis for such processing is performance of the contract.

Processing stakes	Launch and fund 2 Open Calls to select 6 and 7 Bottom-up Projects regarding the development of building blocks for large scale pilots, new analytical tools for the toolbox (prototypes); and the development of new services on existing technologies, respectively.
Controller	PLATOON Project (Project Owner), FundingBox (Data Owner)
Processor(s)	None

Table 26 Open Calls, high-level processing description

Personal Data Management in the Open Calls:

Personal data will be processed in accordance with the GDPR and national and international laws. In accordance with FundingBox's internal policies and the Project's requirements, all personal data will be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

All the personal data will be also processed with the appropriate technical and organizational measures under art. 32 of the GDPR or other generally applicable laws.

Application Data Security

Data will be collected through an online form within the FBOX Platform which will be used during the project´s Open Calls and other administration processes managed by FBA. Data will be deposited and secured in the FBOX platform. The information will be captured through online forms and will be recorded and stored in FBOX Cloud infrastructure as an object database. The information will be accessible through an online Dashboard application and only anonymized data will be downloadable in csv and xls formats. Only authorized users will be allowed to access the data sets via authentication. The FBOX platform applies technological and organizational measures to secure processing of personal data against publishing to unauthorized persons, processing in violation of the law and change, loss, damage, or destruction, including:

- Information security: SSL (Secure Socket Layer) certificates are applied. In order to ensure the appropriate level of security, the password for the account will exist on the platform only in a coded form. Registration on and logging in to the platform proceeds in a secure https connection. Use of password to access data sets: the FBOX platform offers 4 different access levels/roles (administrators, developers, evaluators and invitees) to secure access to data by unauthorized users. Communication between the User's device and the servers will be encoded using the SSL protocol.
- Options for reading data: the platform offers the possibility to make data available in a read-only or downloadable format, hindering the access to information by unauthorized users. Once

an Open Call finishes information is archived, so it's no longer publicly accessible, only administrators will have access to the historic data in a read-only mode.

- Back-up policy: complete and redundant back-ups are done every hour. Moreover, every time a modification is done an older version is saved.
- Accidental deletion or modifications: in case of a catastrophic event that implies the partial or complete deletion of the data sets, the data from the most recent back up will be automatically restored (back-up won't be older than 60 minutes). In case of accidental deletion or modification only the most recent document will be restored, so in case of accidental changes or deletion data can be easily recovered.
- Deletion or modification of data by users: only administrators have the rights to delete or modify the information included in the datasets. Under exceptional circumstances administrators can be given the permission to delete applications (utilities offered by the FBOX platform) but the user responsible of its creation will be notified before doing so.
- Deletion of data by participants in open calls: users having started the application process can withdraw any time using the FBOX platform before the deadline for submission.
- Terms and conditions: the FBOX platform have specific terms of use and conditions that have to be accepted by all users of the platform.
    - FundingBox terms of service: https://fundingbox.com/about/terms
    - FundingBox platform privacy policy https://fundingbox.com/about/privacy

The individual registers of the Open Call and Pilots will be only accessible for evaluation purpose to be done by accredited and authorized evaluators/mentors. Each evaluator/mentor will be granted, with limited access, to a restricted number of registers from the data set. The online access will be awarded for a limited time period, using a secure mode via the authentication process.

The same attention to data protection will be placed in the publication and dissemination of data and analysis in order to maintain the correct balance between scientific explanation and personal data security.

The procedure for data exploitation will be:

1. Storage: The platform will provide a cloud-based environment;
2. Protection: Any databases containing data deemed to be sensitive will be encrypted using the current industry-standard level of encryption.
3. Retention: All personal data collected within open calls will be anonymized and/or destroyed upon completion of the project. In accordance with the General Data Protection Regulation - GDPR, all research data will not be kept for longer than it is needed;
4. Transfer: The exchange of data between partners will be handled by a secure server to ensure maximum security during transmission;
5. Destruction: Data used during the project will be immediately destroyed after analysis. Only data needed for compliance reasons will be kept. Data marked for destruction will be securely deleted using the latest industry-standard techniques.

Upon disclosure of the datasets with the rest of the consortium, each partner is responsible for all obtained data during their processing and acquisition in their own organization. Each partner is obliged to implement appropriate security measures to ensure the confidentiality of the data.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?

Yes: applicant's name, email address, phone number, place of residence/nationality, professional experience, education, and other professional information.	**In place:** Privacy by Design. Data minimization, Technical measures to ensure data integrity, confidentiality, availability, and accountability. **Selected proposals** must follow the ethical and personal data protection requirements, and introduce the security, privacy and sovereignty solutions of PLATOON to prevent intrusion of risks from the external organization, and secure data throughout its full life-cycle.	**Minor** (FBOX platform is currently managed by FundingBox and has a track record of secure operation)

Table 27 High-Level PDP Assessment for LLUC P-2b-01

3.3 PLATOON Solutions

This section will examine the expected solutions and enablers to be developed in the framework of the PLATOON project, carrying out a high-level Personal Data Protection Assessment to identify potential issues vis-à-vis compliance.

3.3.1 Data analytics toolbox

Summary of the activities to be performed:

The PLATOON data analytics toolbox will be a key part of the PLATOON federated platform. Data Analytics toolbox is linked to the Processing part of the PLATOON reference architecture introduced in Section 2. Data Analytics toolbox will be formed of the tools developed in the project by different partners for different pilots. Some of the tools will be open source and free to use and some others will be proprietary and will be used under specific conditions.

The PLATOON platform should be able to manage this repository of centralized and distributed data analytics tools. It must include the functionality to download/connect the different data analytics tools, test them and visualize the results all with a user-friendly interface so that energy domain experts with little coding and data science background can use them. Once the tools are validated and they decide to productionize them, the tools in the data analytics platform must be prepared to be easily integrated into the production system using the concept of containers or microservices. The PLATOON Data Analytics Toolbox and its tools will be defined in WP4.

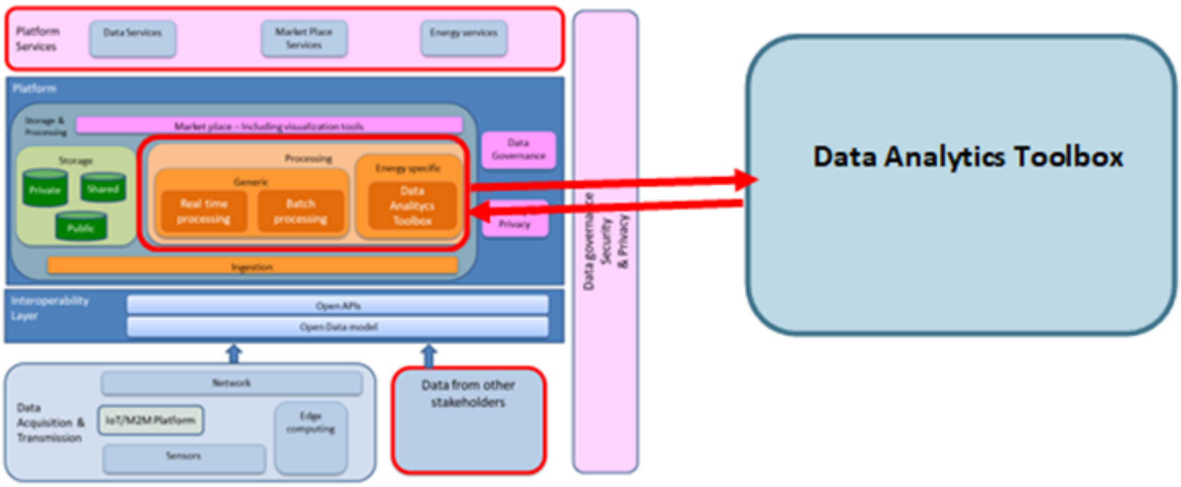


Figure 2 Data Analytics Toolbox in the PLATOON Project Framework

Data sources to be used:

During the project, the data sources that will be used to develop, train, and validate the data analytics tools will be the same datasets available in the different pilots as listed in section 3.1.

Potential for personal data to be compiled:

A potential exists for compilation and processing of datasets which could contain personal data for future applications after the project (beyond the project scope).

Specific actions/methods undertaken by leading partners to prevent use/misuse of personal data:

Data analytics tools process or manipulate input data coming from different data sources. So, the data analytics tools will comply with the data privacy and security requirements established in this document if the input data complies with these requirements. Only for the specific cases identified in this document that require specific actions/methods to prevent use/misuse of personal data, additional data treatment tools (e.g. anonymization/pseudonymization, encryption tools, etc.) will be developed. Whenever is possible, these specific data treatment tools (e.g. anonymization/pseudonymization, encryption tools, etc.) will be developed as an independent standalone module and will be made available as part of the data analytics toolbox so they can be integrated with the rest of the tools for open calls or future applications after the project.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
During PLATOON project: **None**: Only pilot-generated (aggregated) data will be used.	**In place:** Anonymization (Aggregation), Data minimization.	**Negligible,** none of the expected solutions will introduce edge-computing and/or IoT elements which could bring risks to data subjects. Elements added through open calls will have to comply with strict data protection requirements.
Post-project (exploitation): **Potentially (Outside Project-scope)**	**In place:** Privacy by Design, Data minimization. Technical measures to	**Moderate,** depending on the implementation of the solution in a production environment (**outside**

	ensure data integrity, confidentiality, availability, and accountability.	**the scope of the PLATOON project**), the Data Analytics toolbox could handle datasets containing personal data

Table 28 High-Level PDP Assessment for LLUC P-2b-01

3.3.2 Marketplace

Summary of the activities to be performed:

Data is a valuable resource in any digital, data-driven business and is necessary to enable participants to leverage the potential of their data and tools within a secure and trusted business ecosystem. The PLATOON federated platform must enable the exploitation of digital services (both data and data analytics tools) amongst different stakeholders through the PLATOON Marketplace.

The PLATOON marketplace will be a one-stop-shop that integrates all the services developed in the project by the different partners (additional services from previous projects can also be made available). Moreover, the services developed as part of the open calls will be available through the marketplace. The marketplace will mainly offer two types of services data services (share of raw and process data) and app services (data analytics tools that can be downloaded and implemented in the partner platform).

The marketplace is a meeting point for service offer and demand and must meet two fundamental requirements to be functional: to cover the suppliers' product catalogue (offer requirements) and to be a reference for customers (demand requirement). A well-designed Marketplace for the providers but is not known to the user will fall as inefficient as it is known, but what is advertised is not helpful for the customer.

The PLATOON marketplace will be designed in detail and developed in WP3 (T3.4).

Data sources to be used:

The specific datasets that will be made available in the marketplace and the specific conditions under which they will be made available still needs to be defined. This is part of the exploitation plan of the project which is still an ongoing task. During the scope of the project, it is envisioned that the only datasets to be used in the PLATOON marketplace are those associated with the Pilots, for which no personal data will be used.

Apart from the actual datasets also some of the developed data analytics tools will be made available in the PLATOON marketplace. Each of the dataset or data analytics tools will have an associated information containing the contact details of the owner of these datasets/data analytics tools.

Potential for personal data to be compiled in the context of the open calls:

During the open calls or for future applications after the project other datasets might be made available in the PLATOON marketplace that might potentially contain personal data.

Specific actions/methods undertaken by leading partners to prevent use/misuse of personal data:

The datasets that are made available in the PLATOON marketplace should undergo a specific analysis to o prevent use/misuse of personal data. Whenever applies specific anonymization/pseudonymization, encryption actions need to be applied to the datasets before making them available in the PLATOON marketplace.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
During PLATOON project: **None**: Only pilot-generated (aggregated) data will be used.	**In place:** Anonymization (Aggregation), Data minimization, access-right management, data security requirements	**Negligible,** none of the expected solutions will introduce edge-computing and/or IoT elements which could bring risks to data subjects. Elements added through open calls will have to comply with strict data protection requirements.
Post-project (exploitation): **Potentially** (**Outside Project-scope**)	**In place:** Privacy by Design, Data minimization, technical measures to ensure data integrity, confidentiality, availability, and accountability.	**Moderate,** depending on the implementation of the solution in a production environment (**outside the scope of the PLATOON project**), the Marketplace could handle datasets containing personal data.

Table 29 High-Level PDP Assessment for LLUC P-2b-01

3.3.3 Edge computing tools

Summary of the activities to be performed:

The Edge Computing is linked to the Data Acquisition and Transmission part of the PLATOON reference architecture introduced in D.1.3 Section 2. The foundation of edge computing focuses on specific deployment models that aim at balancing among data processing workload, communication channel bandwidth, and guaranteed responsiveness of critical applications.
Edge Computing is a distributed topology where the information processing is placed closer to the things or people that produce and / or consume the information for fast service delivery.
The traditional models of processing and storing data either in the centralized, on-premise location or in the cloud is for numerous applications becoming too costly as well as critical in terms of delay and responsiveness to meet the requirements of particular use cases. Lately this has motivated the enforcement of edge computing approach that facilitates the processing of data closer to the source.
The architectures based on Edge Computing, try to solve two important well-known problems that have arisen in the deployment of the traditional IoT (i) the volume problem of information and (ii) the latency problem in the assisted or automatic decision.

Data sources to be used:

During the project, the data sources used to develop, train, and validate the data analytics tools will be the same datasets available in the different pilots as listed in section 3.1.

Potential for personal data to be compiled in the context of the open calls:

During the open calls or for future applications after the project, other datasets might be made available in the PLATOON marketplace that might potentially contain personal data.

Specific actions/methods undertaken by leading partners to prevent use/misuse of personal data:

Edge computing devices or manipulate input data coming from different data sources/sensors directly at the edge before sending it to the cloud or on-premise infrastructure. So, the edge computing solutions will comply with the data privacy and security requirements established in this document if the input data complies with these requirements.

Unless otherwise stated from the analysis made in section 3.1 we will assume that the raw data complies with the data privacy requirements stated in this document. Only for the specific cases identified in this document that require specific actions/methods to prevent use/misuse of personal data, specific data treatment tools (e.g. anonymization/pseudonymization, encryption tools, etc.) will be developed and implemented directly at the edge computing devices. Whenever is possible, the same data treatment tools (e.g. anonymization/pseudonymization, encryption tools, etc.) developed for other applications and available and that is part of the data analytics toolbox will be implemented in the edge computing devices.

Personal Data Involved?	Implementation of Technical and Organizational PDP Safeguards?	Risks to Rights and Freedoms of Data Subjects?
During PLATOON project: **None**: Only pilot-generated (aggregated) data will be used.	**In place:** Anonymization (Aggregation), Data minimization, access-right management, data security requirements	**Negligible**, none of the expected solutions will introduce edge-computing and/or IoT elements which could bring risks to data subjects. Elements added through open calls will have to comply with strict data protection requirements.
Post-project (exploitation): **Potentially** (**Outside Project-scope**)	**In place:** Privacy by Design, Data minimization, technical measures to ensure data integrity, confidentiality, availability, and accountability.	**Moderate,** depending on the implementation of the solution in a production environment (**outside the scope of the PLATOON project**), the Edge computing tools could involve devices that could collect could handle datasets containing personal data.

Table 30 High-Level PDP Assessment for LLUC P-2b-01

4 Guideline Specification

This section introduces both the functional requirements identified for personal data protection and security and compliments them through a set of guidelines to be considered by all partners throughout the project. Compliance with both actions will be validated throughout Task 3.5 and reported in Task 10.4.

4.1 Requirements

As specified both in the PLATOON DoA and Deliverable 1.2, have identified 12 functional requirements which should be introduced by the project's components, namely:

Req. ID	Description	Req. Group	Req. Type	WPs	Mandatory/ Optional	Pilot Specific /General	Specified in the DoA
12026 **Data Anonymization**	As a PLATOON Data Provider, I want personal data to be anonymized so that I comply with GDPR.	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12027 **Data Pseudonymization**	As a PLATOON Data provider, I want personal data aggregated so that I keep confidential critical business keys.	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12028 **Outbound Security**	As Data Provider, I want companies that are going to have access to data, to meet certain minimum security requirements, so that I can be sure that my data is going to be safe outside my system and that GDPR is going to be complied with	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12029 **Inbound Security**	As Data Consumer, I want the companies that are going to provide me data to meet security requirements so that they do not create cybersecurity threats to my system.	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12030 **Data Protection by Default**	As Data Consumer, I want to know the specific data privacy and usage requirements so that I can be sure to	Data Exchange / Security	Functional	All	Mandatory	General	Yes

	comply with GDPR and only use the data sticking to them.						
12031 **Data Sovereignty**	As a Data Consumer, I want to be sure that the companies that provide the data I am going to use meet ownership and sovereignty requirements, so that I have the permission to use data (e.g. data has been retrieved legally, not stolen).	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12032 **Data Quality and Provenance Verification**	As a Data Consumer, I want to be sure that the companies that provide the data meet quality and provenance requirements (original source and all the subsequent transformations), so that I can be sure that the models I develop based on the data are going to perform well when applied to other datasets.	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12033 **Third-party Certification**	As Data Provider/Consumer and App Provider/Consumer, I want to be part of an ecosystem where all the stakeholders meet data quality, security and privacy requirements, so that I don´t have to check them every time I want to create a new data connection.	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12034 **Data Encryption**	As a Data Provider, I want my data to be encrypted every time it is sent to a Data Consumer, so that were there to be a malicious attack and the data is intercepted, they cannot extract any valuable	Data Exchange / Security	Functional	All	Mandatory	General	Yes

	information from my data.						
12035 **Consent Management**	As a PLATOON Data Provider/Consumer, I want to manage consent over personal data, so that I will be able to manage who can access and process my personal data.	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12036 **Access control**	As a PLATOON Data Provider/App Provider/Service Provider, I want to access control functionalities so that only authenticated and authorized people can access the data/services.	Data Exchange / Security	Functional	All	Mandatory	General	Yes
12037 **Security compliance validation**	As a PLATOON Data Provider/Consumer, I want to comply with state-of-the-art solutions regarding security, so that the data exchange process is secure.	Data Exchange / Security	Functional	All	Mandatory	General	Yes

Table 31 PLATOON Privacy-related functional requirements

4.2 Guidelines

The following guidelines seek to facilitate compliance, by all PLATOON stakeholders, with the requirements identified by D1.2. They will be further enhanced throughout the upcoming months, as the specific plans for implementation of PLATOON are finalized and will be considered, and their implementation reported by T3.3.

4.2.1 Personal Data Protection by Design and by Default (Req. 12030)

The introduction of a requirement to enable safeguards by design and by default as a core principle of personal data protection is a defining characteristic of the GDPR and other recent data protection regulations, and has been integrated into several of the examined normative sources and standards.

Article 25 of the GDPR requires that "*The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*"(European Parliament and European Council 2016).

The overall scope of this requirement includes the introduction of the principles set by the GDPR throughout all stages of the PLATOON project and their implementation by project partners and associated parties in the solutions and enablers developed for the project. The following points will specify the general scope of this implementation[16]:

Lawfulness, fairness, and transparency

As required by the GDPR, PLATOON will only process personal data lawfully, fairly and in a transparent manner in relation to the data subject. To this end, all PLATOON enablers shall ensure that a) personal data is only processed where a lawful ground (legal basis) exists to justify the processing activity; b) the reasonable expectations of individuals with regards to the ways their personal data might be processed are recognized and respected, and the processing activities are balanced in consideration of these expectations; and c) data subjects are correctly informed of the processing activities.

Purpose limitation

As set out by article 5 of the GDPR, PLATOON partners, enablers and solutions shall process personal data only for legitimate, specific, explicit, predetermined purposes disclosed with the data subject at the time of the collection of data, with no additional processing activities purposes.

Data minimization and storage limitation

All PLATOON technologies, solutions and enablers should be designed to minimize the collection of personal data, provide privacy-protective default settings and ensure that data subjects are well informed and have the option to easily modify configurations associated with their personal data.

Accuracy, integrity, and confidentiality

Whenever personal data is collected or processed (particularly vis-à-vis the Open Calls) in the context of PLATOON, partners involved shall ensure that data is kept updated and that the accuracy of the data is reviewed periodically. Furthermore, as noted in point 8.2.3, all partners shall introduce technical measures to ensure the integrity, confidentiality and accessibility of the data to be used in the project (including compliance actions for the integration of the IDS standard in their systems).

Accountability

PLATOON partners shall ensure their processes and/or services are accountable through both internal policies and mechanisms aimed at generating supporting documentation vis-à-vis compliance with relevant personal data protection requirements, and through the communication of processing activities to the PLATOON DPO.

4.2.2 Data Anonymization, Pseudonymization and Retention Compliance (Req. 12026, 12027)

Anonymization

As previously specified, the dispositions of the Personal Data Protection regulations and standards examined do not apply to anonymized data as long as the controller is able to demonstrate that they are not able to identify the data subjects (non-identifiability)[17]. To this end, it is recommended that no

[16] Whenever a partner or associated party is in doubt with regards to the implementation mechanisms, the PLATOON project DPO will be available for consultation and/or further specification.

[17] De-identification is a "General term for any process of removing the association between a set of identifying data and the data subject" (International Organization for Standardization 2008). The EDPB recalls that the principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

data is disclosed by Project partners unless it is anonymized (data masking, data swapping, generalization, data perturbation, etc.).

Pseudonymization

Whenever anonymization is not possible, "Other techniques such as pseudonymization[18] can help minimize the risks generated by the data processing, taking into account that in most cases, directly identifiable data are not necessary to achieve the purpose of the processing (…) Pseudonymization, if reinforced by security safeguards, improves the protection of personal data by reducing the risks of misuse. Pseudonymization is reversible, unlike anonymization, and is considered as personal data subject to the GDPR" (EDPB 2020). In the context of PLATOON pilots, partners should, at minimum, ensure that the data captured from sensors are aggregated to a sufficient extent that no identification with individual persons may be carried out.

Data Retention compliance

Project partners shall establish rational data retention periods for the storage of personal data, however, as a baseline no PLATOON-related personal data shall be kept beyond the end of the project. Furthermore, they all recognize that upon its expiration, data should be erased or de-identified. Unnecessary personal data should be erased by the system without undue delays. All entities, service providers and data controllers related to future PLATOON activities should utilize reasonable or non-extensive data retention periods and integrate necessary technical measures to ensure that unnecessary personal data are neither requested nor registered (principles of storage limitation and data minimization). Furthermore, technical methods should be implemented to ensure that data is effectively deleted, and the process followed should be transparent towards end-users.

4.2.3 Data Security (Outbound & Inbound) (Reqs. 12028, 12029)

All members of the PLATOON recognize the intrinsic connection between security and personal data protection activities and the importance of coordinating technical, contractual, and organizational actions to reduce the risk for both the organizations and the data subjects. PLATOON will protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access through the implementation of technical and organizational measures as required by article 32 of the GDPR.

While the planned actions to be performed during the PLATOON project do not envision processing of personal data for experimental purposes, all PLATOON enablers shall introduce measures to ensure the Authenticity, Integrity, Availability, Confidentiality, Accountability of the processed datasets. This is particularly true whenever the enablers or solutions expressly compile, process and/or disclose personal data (e.g. the Open Calls), where the controller and processor responsibilities will be clearly specified to ensure sufficient protection of the rights and freedoms of the data subjects.

A broad set of data security actions should be undertaken by all PLATOON project partners to ensure the security of the communications (both inbound and outbound) undertaken by the platforms. The specific security requirements have been specified throughout other tasks in this work package: As noted in D1.3, "The PLATOON federated platform must comply with industry cybersecurity standards to ensure that system is immune against malicious attacks. Therefore, the following security requirements must be ensured at different levels: at the device, communication, and user levels:

- At the device level, only those devices/sub-systems that have the required authorization can connect, for which there are security tokens that work as a key and are renewed periodically.
- At the communication level, sensitive information will be exchanged via encrypted channels to protect confidentiality in case there may be a capture of network traffic.

[18] Pseudonymization consists of replacing directly identifying personal data by a non-signifying pseudonym. This can be done by, for example, using a secret-key hash algorithm (EDPB, 2020, pp. 16–17).

- At the user level, roles and access permissions will be defined so that only the appropriate people can use the systems in the permitted functionalities."

Data collected throughout the project will be kept secure. All partners shall implement technical and organizational measures to protect the physical and digital infrastructure used[19]. Compiled datasets will only be used for analysis and development purposes related to the project and will be protected according to the procedures for privacy and intellectual property rights defined in the consortium agreement.

Additional specific requirements to be followed by all stakeholders will continue to be clarified by the PLATOON consortium as further implementation actions are agreed upon.

The following points specify additional elements that should be considered by all partners to ensure that the security activities undertaken comply with the GDPR requirements:

Identification of data categories

The GDPR recognizes the existence of diverse categories of personal data, which are subject to different levels of normative protection. Sensitive or special categories of personal data are recognized and granted additional protection, likewise, non-personal or anonymized data is not subject to protection and can be transferred, as necessary. In light of this perspective, PLATOON project partners, enablers, solutions and associated stakeholders should especially ensure the protection of special categories of personal data as defined in art. 9 GDPR, particularly traffic [20]location data[21], and data that could reveal offences. To this end, particular care will be taken during the pilot implementation and the Open Call process to align the activities in collaboration with the Project DPO.

Periodic update and review of privacy and security measures

According to this requirement, stakeholders involved in future PLATOON activities should have policies in place to ensure the periodic update and review of the privacy measures, policies and mechanisms to ensure their effectiveness. This requirement is closely associated with the need to generate records of processing activities, data breaches and other events, to enable their audit and cross-verification (The developed systems should be able to demonstrate their compliance with the GDPR through the introduction of logging systems).

4.2.1 Data Sovereignty, Quality and Provenance Verification (Reqs. 12031, 12032)

As defined in PLATOON D1.2: "Data is a valuable resource in any digital, data-driven business and is necessary to enable participants to leverage the potential of their data within a secure and trusted business ecosystem. In a nutshell, Data Governance is concerned with data lifecycle management decisions that ensure the safe, fair and secure (determined by pre-defined rules, legislative

[19] Access Control List (ACL), firewall and Unified Threat Management (UTM) system to restrict access and protect the machines. To mitigate the threat posed by the highly unlikely accidental disclosure of data, data obfuscation techniques shall be implemented to make it difficult to utilize such data. Depending upon the security needs of the database, partners shall consider the following techniques: cross-tabulation (spreading data over numerous databases using different keys), data swapping (replacing values in one field with those from another) and salting (adding algorithmically controlled data pieces to stored data values).

[20] Traffic data is defined by the ePrivacy Directive as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication". The ePrivacy Directive explicitly limits the conditions in which traffic data may be processed, with the upcoming entry into force of the ePrivacy Regulation, it is highly likely that the protection granted to traffic data will be enhanced.

[21] In a similar manner as the preceding point, location data can easily contain or indicate special categories of personal data, and must, for this reason, be granted particular protection by PLATOON Project partners, who shall, alongside other relevant stakeholders, be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing.

requirements, etc.) handling of data within and across a network of nodes over which data is passed on to fulfil pre-identified data value chains. In a data ecosystem that involves data exchange between distinct entities to fulfil such data value chains, as in the case of the PLATOON use-cases and the envisioned energy marketplace, Data Governance shapes the foundations of the architecture (e.g. decentralized, centralized or hybrids) and therefore requirements need to be defined and agreed on early on in the project.

Data Governance models define a framework of decision-making rights and processes with regard to the definition, creation, processing, and use of data. As PLATOON has identified the International Data Spaces (IDS) as the of-choice 'de facto' standard for data sharing ecosystems, the project will adhere to the IDS governance model, which governs and determines usage rights of data exchanged within IDS-compliant ecosystems." All systems developed in the framework of PLATOON and associated enablers should be designed to account for and conform to the IDS reference architecture.

4.2.2 Data Encryption (Req. 12034)

All personal data should be encrypted whenever it is stored or transferred. A strong encryption mechanism[22] should be selected to fulfil this requirement, including the adoption of state-of-the-art encryption algorithms and encryption key management, renewal and protection; device authentication, integrity verification (e.g. by hashing) and usage of reliable user authentication techniques.

4.2.3 Consent Management and Data Subject Right Compliance (Req. 12035)

The GDPR and standards like ISO 27701 recognize several rights to data subjects, including rights of access, rectification, opposition, and deletion of personal data. This requirement aims to fulfil these, with the consideration of some additional particularities:

a) The data subjects are to be informed as soon as possible after a breach to their personal data has taken place.
b) The system upon which rights of access are exercised must be available as soon as possible after facing a data breach to ensure that the data subject remains in control of their personal data.
c) All necessary measures should be incorporated to ensure that if the data subject requests the deletion of its data, any controllers or processors who possess copies of the information must be informed and asked to comply with the request.

The following points detail relevant elements vis-à-vis data subject right compliance to be considered by all PLATOON stakeholders when carrying out relevant activities.

The right to be informed

The systems developed in the framework of PLATOON and associated technical security mechanisms should enable its administrators to identify potential breaches to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed as required by articles 33 and 34 of the GDPR. The PLATOON partners and associated service providers should keep track and inform data controllers of breaches to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, thus enabling data controllers to take breach mitigation measures, and if required by law, inform the competent Data Protection Authorities and concerned data subjects of the situation.

[22] Cryptographic protocols: TLS, IPsec, Kerberos, PPP with ECP, ZRTP, etc.

The right of access

The systems developed in the framework of PLATOON and associated technical security mechanisms should enable the data controllers in providing to every data subject, without excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed and information as to: the purposes of the processing; the categories of data concerned; the recipients to whom the data are disclosed; the envisaged period of storage for the data; and the existence of automated decision-making processes within the system. The legal source of this requirement is article 15 of the GDPR.

The right to rectification

Personal data which are inaccurate or incomplete, having regard to the purposes for which they were collected or processed, will be erased or rectified as set out by article 5 of the GDPR.

The right to erasure

The PLATOON platform must ensure that the right of erasure exercised by data subjects towards the data controller is enforced, when the conditions set out by article 17 of the GDPR are met.

The right to restrict processing

Data subjects are granted the right to restrict the processing of their personal data as an alternative to the erasure of their data. PLATOON platform, enablers and solutions shall consider this possibility and enable the performance of such restrictions whenever necessary.

The right to data portability

As detailed by article 20 of the GDPR, the PLATOON platform must be able to support the data controller in responding to requests for data portability lodged by the data subjects. This entails that the data subject shall receive the data in a structured, commonly used and machine-readable format.

The right to object

Data subjects are granted the right to object to the processing of their personal data at any time for either all or specific purposes. The scope and applicability of this right is limited in the expected activities of PLATOON (see GDPR Art. 21(4) and 89(1)). PLATOON platform, enablers and solutions shall consider this possibility and enable administrators to implement the request.

Rights in relation to automated decision making and profiling.

The GDPR recognizes the rights of data subjects to not be negatively impacted by automated individual decisions affecting data subjects based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. The PLATOON ecosystem, and particularly the enablers to be developed in the framework of the Pilots (e.g. the tool to detect non-technical losses) will account for this right and introduce sufficient safeguards (including human oversight) in a future implementation beyond the project scope.

4.2.4 Access control (Req. 12036)

In order to ensure compliance with the security requirement of non-refutability and accountability, and to guarantee compliance with the relevant data protection dispositions, the EDPB guidelines recommend the generation and maintenance of history logs of any access to the information system, e.g. going back six months as a maximum period, in order to enable the origin of any potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies. These logs should be protected by strong security mechanisms (such as encryption, physical safeguards, and redundancies).

To ensure non-refutability, the solutions developed in the context of the PLATOON ecosystem will authenticate and appropriately authorize the identities accessing the platforms before enabling users to use them. Where necessary (e.g. when the system is used to process health data), strong authentication (e.g. two-factor authentication, double opt-in, biometric recognition, etc.) methods must be supported. Personal authentication credentials shall be de-activated if they have not been used for at least six months (except in case of technical authorization).

4.2.5 Third-party Certification & Security compliance validation (Req. 12033 & 12037)

As per the IDS governance model described in D1.2, to ensure trust in the PLATOON ecosystem, all Data Providers/Consumers, App Providers, Data Apps should undergo certification from a Certification body. While it is up to the Steering Committee to specify who can fulfil this role in the envisaged PLATOON Energy Data Marketplace, both during (e.g., Steering Committee fulfils the role) the project and after the end of the project (e.g. appropriate independent entities that will by then be available)[23], from a Personal Data Protection perspective, a similar approach should be considered in alignment with Requirements 12033 and 12037.

Personal Data Protection Certification

As previously specified, the intricate set of technical and functional requirements relevant for the PLATOON project, will require a solution to generate trust in the PLATOON ecosystem. Certification has been a historic solution to enable the globalization and interoperability of technologies. By ensuring conformity criteria and incorporating these into the business practices, players in the market can ensure their products and services will be easily adopted regardless of the final location of the deployment. Personal data protection regulations, however, presents a complication to this situation, as they include both technical and organizational requirements and even incorporate security requirements and best practices which have traditionally been outside of the scope of most national legal frameworks.

As defined before, the European approach to Personal Data Protection presents many such challenges to the deployment of innovative technologies in a globalized environment, and lack of compliance (or incomplete compliance) with such requirements is likely to impair adoption, impact and exploitation of the solutions and enablers developed in the PLATOON project.

A potential solution to this situation can, however, be found in voluntary GDPR-specific certification schemes, which have been developed and approved in accordance with Art. 42 and 43 of the GDPR to "demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries (…)" (European Parliament 2016a).

Europrivacy, a certification scheme developed through the Horizon 2020 European research programme with financial support from the European Commission and Switzerland may present a potential solution for the PLATOON project. Europrivacy was developed through a sequence of European research projects, including: EAR-IT (2012-2014 on privacy risk assessment methodology), Privacy Flag (2015-2018 on certification scheme design), and ANASTACIA (2017-2019 on authenticated certificates). It was also extended and used in the context of Synchronicity, the European Large-Scale Pilot on Internet of Things for Smart Cities, to assess the compliance of smart city deployments with the GDPR.

It was co-created thanks to several European research partners committed to promote personal data protection and to support the implementation of the GDPR. Europrivacy is managed by the European

[23] The IDS Association is working on providing Certification services for IDS-compliant data spaces. However, it is not possible to foresee the state or maturity of these services by the project's end or whether they are appropriate for the PLATOON data marketplace.

Centre for Certification and Privacy (ECCP) in Luxembourg under the guidance of an international board of experts in data protection. ECCP has been granted the status of research center by the authorities of Luxembourg and will keep continuous and close cooperation with the European research programme to maintain a high level of reliability of its certification scheme by leveraging on the European research community and a network of seasoned experts in data protection from all over Europe and beyond.

Europrivacy is a European certification scheme on data protection that encompasses the European General Data Protection Regulation and can easily be extended to include complementary national and domain-specific obligations, which makes it particularly relevant in the context of 5G-DRIVE. It has been designed to be comprehensive and capable of assessing a large scope of data processing activities by complementing its core list of checks and controls with complementary ones according to the Target of Evaluation. While its focus is on data processing activities (following the required approach by EDPB), its dual compliance with ISO/IEC 17065 and 17021-1 (where applicable) enables Europrivacy to assess data processing in the context of services, products, and information management systems.

In order to assess the potential applicability of Europrivacy towards the PLATOON ecosystem, it is recommended that Task 3.3 and all tasks associated with standardization build upon the Europrivacy Scheme model to develop tailored criteria that meet the security and data protection requirements of the PLATOON ecosystem and reach a consensus with the project partners to identify whether broad adoption of this certification is possible.

5 Discussion and conclusion

This report has presented the initial evaluation of the legal and ethical requirements that are relevant to the PLATOON project. At the time of preparation of this Deliverable, no critical ethical related issues can be identified. The Project remains committed towards carrying out a permanent ethical evaluation and will closely follow the H2020 Ethics Appraisal Procedure for the evaluation of applications to the Open Calls.

From a personal data protection perspective, no critical issues can be identified at this stage of the project. This deliverable has carried out a high-level personal data protection assessment for PLATOON High/Low-level use-cases, identifying minimal concerns due to the general lack of personal data processing activities in the expected PLATOON pilots. A similar situation has been identified with regards to the PLATOON Open Calls, where a solid personal data protection strategy has been set in place by FundingBox (and which is complemented by the guidelines described in this document).

The work done throughout this document shall serve as a baseline for the continuous Legal and Ethics support actions to be carried out throughout the project. Section 3 performed a comparative analysis of the national guidelines on DPIA and identified the potential for personal data processing activities to take place through the developed solutions after the end of the PLATOON project. While neither the EDPB nor the nationally defined DPIA criteria are met by these processing activities, it is recommended that DPIAs are performed in line with the description of Task 3.5, and their results considered by Task 8.3 to maximize the potential for exploitation, sustainability and large-scale uptake beyond the project's lifetime.

A Personal Data Protection by Design and by Default approach will be adopted for the rest of the PLATOON enablers, and solutions (particularly towards the data analytics toolbox, the Marketplace and the Edge Computing Tools), which will mitigate any remaining risk to the rights and freedoms of data subjects, especially when paired with the nature of the datasets to be used in the Project. This approach will also serve to mitigate potential issues that have been identified as potentially relevant beyond the project scope.

Lastly, the document presents a set of guidelines on GDPR compliance based on the functional requirements identified in D1.2, which have been addressed expressly. These guidelines should be considered by all PLATOON stakeholders throughout the remainder of the project, and their implementation should be closely monitored by Tasks 3.3, 3.5 and 10.4. As a final consideration, it is recommended that the PLATOON Steering Committee considers Personal Data Protection certifications as a trust-enhancing method in line with the expected IDS certifications recommended by D1.2.

6 References

- Andrea Jellinek (2019) Statement 3/2019 on an ePrivacy Regulation
- Belgian Data Protection Authority - List of processing operations requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679 (2019) https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/01_2019_SG.pdf
- Belgian Parliament - Law establishing the Data Protection Authority (2018) https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Act_establishing_DPA_30_07_2018.pdf
- Belgian Parliament - Law establishing the information security committee and amending various laws concerning the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to processing personal data and the free movement of such data, and repealing Directive 95/46 / EC
- Belgian Parliament - Law regulating the installation and use of surveillance cameras
- Belgian Parliament - Law relating to the protection of individuals with regard to the processing of personal data (2018) https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Act_30_07_2018_final.pdf
- EDPB - Guidelines 05/2020 on consent under Regulation 2016/679 (2020) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
- EDPB - Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation (2018) https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-12018-certification-and-identifying-certification_en
- EDPB - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation (2019) https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22019-processing-personal-data-under-article-61b_en
- EDPB - Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation (2018) https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en
- EDPB - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01
- EDPB - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 (2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- EDPB - Guidelines on Data Protection Officers ('DPO'), WP243 rev.01 (2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

- EDPB - Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01 (2016) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
- EDPB - Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01 (2016) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233
- EDPB - Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (2016) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
- EDPB (2020) Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications
- European Commission (2017) Proposal for Regulation on Privacy and Electronic Communication
- European Council (2014) Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- European Parliament (2016a) General Data Protection Regulation
- European Parliament (2016b) Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
- European Parliament, European Council (2016) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- French Data Protection Authority - List of processing operations exempt from data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679 (2019) https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000039249797
- French Parliament - French Data Protection Act (2019) https://www.cnil.fr/fr/la-loi-informatique-et-libertes
- International Organization for Standardization (2008) ISO/TS 25237:2008 Health informatics -- Pseudonymization
- IONOS (2020) ePrivacy Regulation: About the EU’s privacy policy. In: IONOS Digitalguide. https://www.ionos.com/digitalguide/websites/digital-law/eprivacy-regulation-about-the-eus-privacy-policy/. Accessed 12 Mar 2020
- Italian Data Protection Authority - List of processing operations requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679 (2018) https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9059358
- Italian Parliament - Personal Data Protection Code https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.2
- Serbian Data Protection Autority - List of processing activities requiring a data protection impact assessment (DPIA) (2019) https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/zastitapodataka/Odlukaprocenauticaja.pdf
- Serbian Parliament - Law on Personal Data Protection "Official Gazette of RS" no. 87/2018 of 13.11.2018 (2018) https://www.poverenik.rs/images/stories/dokumentacija-nova/zakoni/ZZPLnovembar2018/ZZPLnovembar2018.doc

- Serbian Parliament - Law on ratification of the Convention for the protection of persons with respect to the automatic processing of personal data (2009) https://www.poverenik.rs/images/stories/dokumentacija-nova/konvencijacir.doc
- Spanish Data Protection Authority - List of processing operations not requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679 (2019) https://www.aepd.es/sites/default/files/2019-09/ListaDPIA-35-5-Ingles.pdf
- Spanish Parliament - General Telecommunications Law 9/2014, of May 9. (2014) https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950
- Spanish Parliament - Law 34/2002, of July 11, on services of the Information Society and Electronic Commerce. (2002) https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
- Spanish Parliament - Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (2018) https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673
- Tsakalakis N, Stalla-Bourdillon S, O'Hara K (2017) Identity Assurance in the UK: technical implementation and legal implications under eIDAS. JWS 3:32–46 . https://doi.org/10.1561/106.00000010