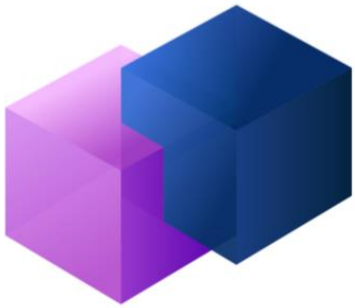
The PARITY project has received funding from the EU's Horizon 2020 research and innovation programme under grant agreement No 864319




| | |
|---|---|
| Project Acronym: | **PARITY** |
| Project Full Title: | **Pro-sumer AwaRe, Transactive Markets for Valorization of Distributed flexibilITY enabled by Smart Energy Contracts** |
| Grant Agreement: | **846319** |
| Project Duration: | **42 months (01/10/2019 – 31/03/2023)** |

# DELIVERABLE D3.4
# Report on Specifications to Ensure Privacy and Security

| | |
|---|---|
| Work Package: | **WP3 – Use Cases, Requirements and System Architecture Definition** |
| Task: | **T3.4 – PARITY Privacy & Security Framework Specifications** |
| Document Status: | **Final v1** |
| File Name: | **PARITY_D3.4_Report on specifications to ensure privacy and security_R1_V1.0** |
| Due Date: | **September 2020** |
| Submission Date: | **November 2020** |
| Lead Beneficiary: | **CERTH** |

| **Dissemination Level** | |
|---|---|
| Public | X |
| Confidential, only for members of the Consortium (including the Commission Services) | |

The PARITY project has received funding from the EU's Horizon 2020 research and innovation programme under grant agreement No 864319

# Authors List

| Leading Author | | | | |
|---|---|---|---|---|
| First Name | | Last Name | Beneficiary | Contact e-mail |
| Stylianos | | Zikos | CERTH | szikos@iti.gr |
| Co-Author(s) | | | | |
| # | First Name | Last Name | Beneficiary | Contact e-mail |
| 1 | Christos | Timplalexis | CERTH | ctimplalexis@iti.gr |
| 2 | Kostas | Afentoulis | CERTH | afentoul@iti.gr |
| 3 | Christos | Malavazos | HYPERTECH | c.malavazos@hypertech.gr |
| 4 | Antonis | Papanikolaou | HYPERTECH | a.papanikolaou@hypertech.gr |
| 5 | Kostas | Kompos | HYPERTECH | k.kompos@hypertech.gr |
| 6 | Giorgos | Fiotakis | HYPERTECH | g.fiotakis@hypertech.gr |
| 7 | Panagiotis | Andriopoulos | QUE | panos@que-tech.com |
| 8 | Chara | Zografou | QUE | ch.zografou@que-tech.com |
| 9 | Davide | Rivola | HIVE | davide.rivola@hivepower.tech |
| 10 | Davide | Strepparava | SUPSI | davide.strepparava@supsi.ch |
| 11 | Cruz | Borges | DEUSTO | cruz.borges@deusto.es |
| 12 | Camilla | Borges Rampinelli | E7 | Camilla.BorgesRampinelli@e-sieben.at |
| 13 | Andreas | Muñoz Zuara | CIRCE | amunoz@ficirce.es |

# Reviewers List

| Reviewers | | | |
|---|---|---|---|
| First Name | Last Name | Beneficiary | Contact e-mail |
| Esteban Damián | Gutiérrez Mlot | CIRCE | edgutierrez@fcirce.es |
| Guntram | Pressmair | E7 | guntram.pressmair@e-sieben.at |

# Version History

| Version | Author | Date | Status |
|---|---|---|---|
| 0.1 | Stylianos Zikos, CERTH | March 27, 2020 | Initial draft (TOC) |
| 0.2 | Stylianos Zikos, CERTH | July 7, 2020 | Initial content added |
| 0.4 | Stylianos Zikos, CERTH | September 7, 2020 | Content about methodology added |
| 0.8 | Stylianos Zikos, CERTH | October 29, 2020 | Measures for privacy and security |
| 0.9 | Stylianos Zikos, CERTH | November 12, 2020 | Final draft for internal review |
| 1.0 | Stylianos Zikos, CERTH | November 27, 2020 | Final version including comments from partners, ready for submission |

# Legal Disclaimer

The PARITY project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864319. The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the Innovation and Networks Executive Agency (INEA) or the European Commission (EC). INEA or the EC are not responsible for any use that may be made of the information contained therein.

# Copyright

# Executive Summary

This document reports the specifications of the PARITY privacy and security framework that will be implemented to the PARITY system. Privacy and security are highly important within the project due to the transactions among different stakeholders, namely the residential and commercial Prosumers, the Aggregator, Market Operator and DSO, as well as the collection and processing of measurement and operation data from devices through the IoT network.

A "privacy by design" approach has been followed by considering data access, transfer and storage issues during the PARITY architecture definition process. Initially, the most critical security and privacy risks have been identified through the Data Protection Impact Assessment (DPIA) that was conducted by each pilot partner. The DPIA document has been created based on templates provided by GDPR and targeting Smart Grid and Smart Metering systems.

Moreover, privacy and security requirements that must be met in order to comply with the GDPR have been identified. Guidelines proposed by organisations and task forces, such as the Smart Grid Task Force, were reviewed and the ones relevant to the project are presented in this report.

GDPR-compliant data handling procedures that will be followed are outlined; however, this report is primarily focused on the privacy and security specifications defined at system level. The security access control framework of PARITY includes measures that will be implemented to protect data from abuse, theft, and loss. These measures involve role-based access control, user authentication and authorization, use of secure communication protocols, and data encryption. With regard to privacy protection, anonymization and pseudonymization will be the key measures that are going to be applied at the IoT platform level and at the LFM level. Lastly, the implementation of the privacy and security measures in each of the main PARITY components, as defined in the architecture design, have been presented in the last section.

# Table of Contents

## List of Figures



## List of Tables

# List of Acronyms and Abbreviations

| Term | Description |
|---|---|
| AES | Advanced Encryption Standard |
| ACL | Access Control List |
| BaaB | Building-as-a-Battery |
| BRP | Balance Responsible Party |
| CA | Certificate Authority |
| DB | Database |
| DBMS | Database Management System |
| DLTs | Distributed Ledger Technologies |
| DoA | Description of the Action |
| DPIA | Data Protection Impact Assessment |
| DSO | Distribution System Operator |
| EEA | European Economic Area |
| EV | Electric Vehicle |
| GDPR | General Data Protection Regulation |
| IML | Information Management Layer |
| IoT | Internet of Things |
| JSON | JavaScript Object Notation |
| LEM | Local Energy Market |
| LFM | Local Flexibility Market |
| OCPI | Open Charging Point Interface |
| OT | Operational Technology |
| OTA | Over-the-Air |
| P2H | Power-to-Heat |
| PII | Personally Identifiable Information |
| RBAC | Role Based Access Control |
| RSA | Rivest–Shamir–Adleman |
| RTU | Remote Terminal Unit |
| SEAC | Security Access Control |
| SGTF | Smart Grid Task Force |
| SSL | Secure Sockets Layer |
| STATCOM | Static synchronous compensator |
| STS | Station-to-Station |
| TLS | Transport Layer Security |
| TSO | Transmission System Operator |
| UI | User Interface |
| UPS | Uninterruptible Power Supply |
| USEF | Universal Smart Energy Framework |
| VPN | Virtual Private Network |
| WP | Work Package |

# 1. INTRODUCTION

The integration of Internet of Things (IoT) and Blockchain technologies will be developed within PARITY, in order to deliver a unique local flexibility management platform. A smart-contract enabled market platform, based on blockchain technology, will facilitate the efficient deployment of local micro-transactions and reward flexibility in a cost-reflective and symmetric manner, through price signals of higher spatio-temporal granularity based on real-time grid operational conditions.

Moreover, by deploying advanced IoT technology, PARITY will offer distributed intelligence and self-learning/self-organization capabilities, orchestrated by cost reflective flexibility market signals generated by the blockchain Local Flexibility Market platform. Within PARITY, DER will form dynamic clusters that essentially comprise self-organized networks of active DER nodes, engaging in real-time aggregated & P2P energy/flexibility transactions.

In addition, the PARITY project aims to enable the set-up and operation of local flexibility markets at the distribution network level via a holistic offering encompassing. For instance, PARITY will enable, blockchain based LEM/LFM platform which will facilitate both peer-to-peer energy/flexibility transactions as well as the sell/purchase of flexibility to Smart Grid actors, and additionally, IoT enabled DER Flexibility management tools - both in a peer-to-peer distributed fashion, but also through a centralized Aggregator. Due to the involvement of various actors that will participate in the LEM and LFM such as the Prosumers, the Aggregator and the DSO, and the need for data exchange and storage of user preferences, grid network parameters and transactions, the requirement for effective data management becomes apparent.

Several terms are used invariably about data management. The most common of these are data protection, data security, and data privacy. The descriptions below elaborate the differences between these terms.

***Data protection***: It encompasses both technical and interactive aspects of data management. It refers to the prevention of the loss, compromise or corruption of digital information [1]. In effect, data protection measures can be divided into two threat categories. These are physical or technical and interactive challenges.

***Data security***: It refers to the protection against physical and technical data management threats. The term data security is often used interchangeably with data protection. As such, Data security refers to the protection against loss or corruption of data. This includes the secure storage and backup of data.

***Data privacy***: Interactive data protection measures cater to data privacy concerns. These measures promote information security by preventing data breaches and compromises. Data privacy is an aspect of data protection that has a wide range of applications and interpretations, and is the main area of data protection that is covered in the GDPR. Data privacy protocols aim at preventing the disclosure of sensitive information to unauthorized parties [2]. They are concerned with regulatory restrictions on how data is collected, processed, stored, shared, used and moved.

The security objectives of energy grids are somewhat different than the ones of other industries [3]. For energy grids, it is of utmost importance that security measures do not affect the availability of the grid. Therefore, the main security objective is availability, followed by integrity. Confidentiality is another security objective. In smart energy systems, there are segments where confidentiality is more important, such as personal data management and market information.

Various strategies have been developed to reduce the risk of data breaches and protect users from fraud. This includes internet security protocols, data protection policies and security technologies such as the blockchain. The blockchain technology, which is used in the PARITY project, provides a secure immutable platform for keeping records and processing transactions.

Special attention has been given on:

- protection of personal data collected at the Prosumer side, and especially those concerning residential Prosumers
- shielding data transfers between devices and components
- compliance with work of Smart Grid Task Force (SGTF) related to data protection (data privacy and security)

## 1.1 Scope and Objectives of the Deliverable

This deliverable deals with data privacy and security risks and measures, which are very important topics for the PARITY project where energy/flexibility transactions are possible through an LFM. This is because various types of data will be collected, such as power consumption data, preferences, devices / EV usage data, and other. In addition, actors with different roles, objectives, and interests are involved, such as Prosumers, Aggregators, and DSO. Therefore, it must be ensured that each actor can have access only to relevant information.

The main objectives of this deliverable are to (a) report the specifications of the PARITY system that have been defined to ensure privacy and security and reduce the risks, and (b) describe the Security Access Control (SEAC) framework that has been developed to protect users' data. To this end, relevant guidelines from Smart Grid Task Force (SGTF) and other associations have been gathered and taken into account, as well as the privacy and security risks, which were identified and collected from each pilot.

A "privacy by design" approach was followed, as data access, transfer and storage issues were considered during the PARITY architecture definition within Task 3.5. "Privacy by design" was introduced by Ann Cavoukian [4] to emphasize that privacy "must ideally become an organization's default mode of operation", and not something to be considered at a late stage. Thus, before the actual software/system development, privacy requirements have to be specified and taken into account. The methodology that was followed for the definition of privacy and security specifications, and SEAC development, is depicted in Figure 1. At the first stage, information collected on the following key points was used as input:

- Privacy and security risks identification
- GDPR and national legislation requirements
- Individual additional privacy and security requirements from pilot partners
- Smart Grid Task Force guidelines on privacy and security

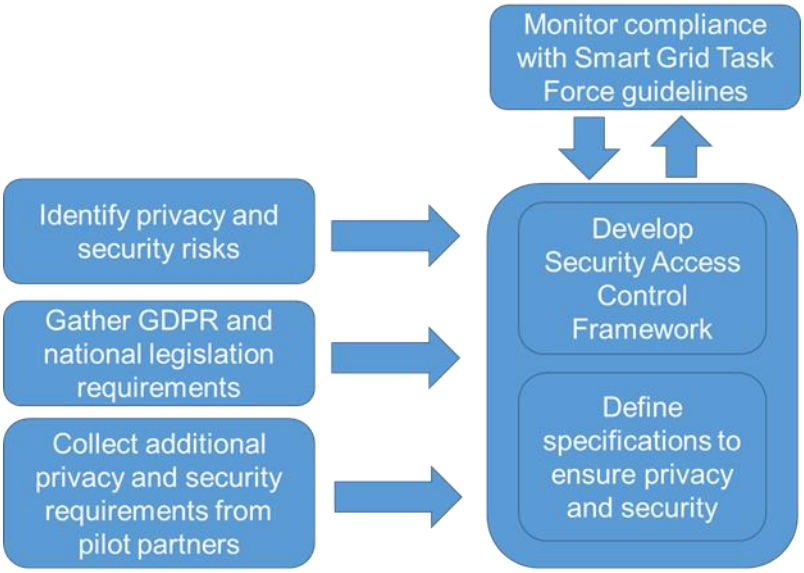



**Figure 1. Methodology for definition of privacy and security specifications, and SEAC development.**

## 1.2 Structure of the Deliverable

The structure of the deliverable is as follows: Section 2 presents an overview on the potential privacy and security challenges that the different actors involved in an LFM may encounter. Section 3 presents the most important regulations related to data privacy and security as defined by GDPR and national laws, as well as guidelines that are proposed by organisations (e.g. SGTF) that are involved in the specifications design of Smart Grids. Security and privacy requirements of PARITY pilots are presented in section 4. These have been derived after the analysis of the security and privacy risks, as documented and prioritized through the DPIA process. Next, section 5 describes the security measures (specifications) that will be implemented and included in the Security Access Control Framework, based on the requirements described in the previous section. Similarly, the privacy specifications are described in section 6. Section 7 presents the way the specifications will be implemented by the relevant PARITY components as defined in the architecture. Finally, the main conclusions of this work are provided in section 8.

## 1.3 Relation to Other Tasks and Deliverables

For carrying out the work and preparing this deliverable, input from the following tasks and deliverables was received:

- Deliverable 1.1 - Ethics Manual that was prepared within Task 1.1 - Ethics Management
- Deliverable 2.2 – Data Management Plan, which is associated with Task 2.1 – Governance, technical coordination and quality assurance, and describes types of data that will be collected and shared
- Deliverable 3.1 – PARITY Business use cases & Requirements associated with Task 3.1 – Elicitation and analysis of business/use cases and requirements for the PARITY tool suite
- Task 3.5 – PARITY System Specifications & Architecture definition

The specifications defined in this deliverable will be taken into account during the development of PARITY components within the tasks of WP5 – Local Flexibility Market Platform, WP6 – Smart Grid Optimization & Management, and WP7 – DER Flexibility Management & Storage-as-a-Service.

# 2. SECURITY AND PRIVACY CHALLENGES

A Local Energy/Flexibility Market involves actors of different roles, therefore their needs with regard to privacy and security may differ. An overview of security and privacy challenges that main actors of a LEM/LFM, i.e. Prosumers, Aggregators, and DSOs, may encounter is provided in this section.

## 2.1 Prosumers

Prosumers, either residential or commercial, procure energy or provide flexibility and in order to accomplish this, their devices and DERs have to be controllable and monitored through an IoT network. Data leaks, intrusions, and data manipulation are common issues that can be the result of inadequate IoT security, affecting Prosumers' privacy and security. DERs' and devices' status information as well as predicted flexibility are usually sent to an Aggregator for more efficient management. However, privacy issues arise since personal information that can reveal Prosumers' behaviour will be available to the Aggregator's system.

## 2.2 Aggregators

Aggregators can interact, apart from the Prosumers, with other actors such as the DSO and BRPs. They need to make sure that no customers' data can be accessed by those actors without permission, and that only necessary data may be provided. Another security challenge Aggregators may encounter is that their systems can become attractive targets to attack, as they collect information from multiple Prosumers.

## 2.3 DSOs

A DSO is responsible for continuously monitoring grid network state and performing management actions when emergency incidents are detected. Moreover, it participates to the LFM market as a flexibility buyer. Even though communication with LFM must be established for performing the flexibility requests and providing local grid status and constraints, DSO system maintains access to confidential information about grid organization and equipment that shall not be published to other actors in the LFM.

# 3. REGULATIONS AND GUIDELINES FOR PRIVACY AND SECURITY

## 3.1 GDPR

The General Data Protection Regulation (GDPR) is a legal framework designed to give EU citizens the power to define how their personal data is used. The guidelines require companies to disclose how they use, store, process and move any personal data collected from individuals in the EU or EEA. The policy applies to any site that attracts visitors from the EU regardless of whether they are based in the region [5]. The policy also gives individuals the right to request for their personal data to be amended or deleted at any time [6].

Below are the definitions of selected terms as they are used in the GDPR and this document.

- Data Subject: Any identifiable individual in the EU.
- Personal Data: Any information directly attributed to an identifiable natural person or data subject.
- Processing: any digitized operation carried out on or using personal data. This includes the collection, storage, transfer, conversion and others.
- Controller: a natural or legal party that determines the purposes and method to proves personal data
- Processor: a natural or legal party that processes personal data under the direction of the controller.

### *3.1.1 Energy consumption data*

Special attention should be given to the protection of energy consumption data that are collected automatically using smart meters. Information about installed equipment combined with information from smart meters can reveal consumption profiles, as well as behaviours and users' preferences. This is an important aspect, especially when residential Prosumers are engaged, as within PARITY project.

A wealth of information can be extracted from the energy usage data generated by smart energy systems, through analytics and predictive profiling. In addition to the use of the smart metering devices, the combined use of other control and monitoring equipment installed in houses, such as environmental and occupancy sensors, climate monitoring/control equipment, and actuators, can give not only a profile of the resident's schedule but also preferences and habits that are important to the resident. On the contrary, individuals and businesses can both benefit from sharing certain privacy sensitive data. For example, common value benefits from data sharing to grid operators and energy service providers include proactive network maintenance, as well as improved operational efficiency and management of assets. In any case, individuals must be aware about the data they share and how these are used by their service providers, and provide their consent on the data collection and processing.

According to USEF, which is compliant with the GDPR, all data on energy consumption are treated as personal data and are subject to a DPIA. Data streams based on necessity, such as public interest or a legal obligation, are separated from those based on consent, such as for value added services [3]. Within PARITY, measures to prevent identification of individual Prosumers by other actors will be implemented to the system. Moreover, processing of personal data collected from sensors will be automated and the output will be utilized by the respective components without displaying unnecessary information to administrator users.

### *3.1.2 Blockchain and GDPR compliance*

Blockchain technology plays a key role in PARITY as it is used for facilitating Local Flexibility Market transactions among participating parties through smart contracts. The blockchain is a decentralized distributed ledger technology (DLT) that offers the secure storage of several types of data. It is an immutable ledger that is accessible anywhere in the world at any time and is not controlled by any central authority.

While the blockchain offers a high degree of data protection, its approach is not directly applicable to the GDPR. The blockchain achieves security through transparency while the GDPR requires the concealment of personal data. Yet, there are several ways in which a middle ground can be reached where blockchains are fully compliant with GDPR policies.

Blockchains consist of information stored in a network of encrypted blocks of data. The technology derives its name from its framework that links blocks of data through chains of complex encryptions. Each block consists of a collection of encrypted data entries. The data is secured using the authors' unique encryption key. It is then certified and encrypted further by a set of validators before it is added to the blockchain. The validators' computers represent nodes on the blockchain network. These validators commit their computational resources to verify the authenticity and validity of each transaction or data entry. New data can only be added to the chain when the acceptable number of validators has verified it. In most systems, data is only added when two-thirds of the validators have verified its authenticity.

Modern Blockchains inherently assume that a third of the participating validators are malicious or faulty. These are referred to as Byzantine Fault Tolerant (BFT) systems. These faults can be caused by computational errors or technical difficulties when validating the data.

The enforcement of GDPR protocols has been particularly challenging for the blockchain and other DLTs. This is because some fundamental blockchain security characteristics limit the implementation of various GDPR protocols. The most challenging of these characteristics are listed below.

- Blockchain data immutability
- Blockchain data distribution
- Blockchain decentralization
- Blockchain data permanence

GDPR compliance on the blockchain needs the alignment of the three core elements. These are the GDPR protocols, the blockchain framework and the personal data in question.

The blockchain features identified as limitations to GDPR compliance are deeply set in the DLT's structure. They are fundamental characteristics that cannot be manipulated without compromising the value of the blockchain.

In the same breath, the GDPR policy is quite comprehensive with little room for manoeuvrability. It is a detailed policy that consists of 99 articles that elaborate its specific applications. Its protocols are designed for application on a wide variety of platforms, both online and offline. Therefore, the GDPR requirements cannot be altered to suit the blockchain limitations.

The only element left to facilitate the integration of GDPR protocols on the blockchain is the personal data submitted for processing. The GDPR policy is only relevant for data that can be used to identify a natural person directly or indirectly [10]. As such, to achieve compliance, the data should be fashioned such that it cannot identify the data subject.

The basic idea of this approach to data management is to separate the data subject's Personally Identifiable Information (PII) from the submitted data set. Once the PII has been removed, the dataset becomes objective. It cannot be attributed to any person either directly or indirectly. This can be achieved through any one of the four methods discussed below.

1. Personal Data Avoidance

2. Personal Data Encryption

3. Personal Data Anonymization

4. Personal Data Pseudonymization

It is important to note that these approaches do not manipulate or infringe any of the GDPR or blockchain protocols. They are all legitimate data management procedures that can be applied safely to various sets of personal data. Data encryption, anonymization and pseudonymization [11] are widely acceptable data masking procedures that have been given special consideration within the GDPR protocols.

*Personal Data Avoidance*: The easiest way to achieve GDPR compliance on the blockchain is to avoid processing personal data. This requires the data subjects, and controllers to be clear on what the GDPR considers personal data. Yet, the omission of all personal data from the blockchain will significantly limit the scope of its operations. A blockchain that exclusively deals with non-personal data may not be practical in today's data economy.

*Personal Data Encryption*: It is possible to encrypt personal data before storing it on the blockchain. The access, amendment and deletion of the personal data can be managed through the data subject's unique encryption keys. However, the blockchain limitations of data permanence and immutability still pose a challenge to this approach. This is because the personal data stored on the blockchain, though encrypted, cannot be altered or deleted. If there is a breach that compromises the data subject's encryption keys, the data can be exploited. In addition, as technology advances, the most versatile encryption keys today may become obsolete in a few years. This means the encrypted personal data stored on the blockchain is always at risk of exposure to some degree.

*Personal Data Anonymization*: Data anonymization is a process that encrypts or removes PII from data sets. It aims to ensure that the data subjects associated with the data sets remain anonymous. Anonymization is a data masking method that is specifically supported by the GDPR policy. However, GDPR-compliant data anonymization is considerably high [11]. The policy requires that any attempt to anonymize personal data should eliminate the risk of re-identification. This means the protocol should go beyond the anonymization of obvious personal data such as names and addresses. Yet, eliminating the risk of data subject re-identification through anonymization can be challenging on the blockchain. To achieve this, the blockchain controller needs to screen all possible data points that can be linked back to an individual. Incomplete anonymization creates still leaves the underlying personal data at risk of exposure. Anonymization on the blockchain is permanent. As such, the data can never be linked back to an individual. While this is a quintessential advantage for GDPR compliance, it creates a challenge for blockchain transparency and validation. The lack of identifiers increases the complexity of data verification and transaction authentication.

*Personal Data Pseudonymization*: Pseudonymization is another effective method of masking personal data on the blockchain. It involves assigning pseudonyms to personal identifiers. This prevents the data from being linked to an identifiable person without using additional information. Through pseudonymization, GDPR policy requires any information that can be attributed to an identifiable person be kept separate from the data sets being processed. It authorizes the controller to apply technical measures within to ensure that the PII cannot be linked to the data subject [10]. The GDPR pseudonymization guidelines apply to all types of organizations that process personal data. Yet, it is uniquely suited for blockchain data masking. This is because the data subject's PII can be maintained off the blockchain while processing personal data. The blockchain controllers can use various mechanisms to create links between the processed data and the personal identifiers where necessary. This approach allows data subjects to access their data on the blockchain through the links provided by the controller without being directly identifiable. GDPR compliance is thus achievable since the personal identifiers and not subject to blockchain limitations. The data subject can modify or erase their personal data without creating new blocks on the chain. Although the personal identifiers are replaced with pseudonyms, the GDPR policy still considers it personal data. Yet, this method enables the controller to prevent the disclosure and distribution of personal data to blockchain validators. Severing the links between PII and processed data minimizes the risk of the data being attributed to an identifiable person. Yet, the data pseudonymization is still reversible even when the additional information on personal identifiers is held off the chain. The blockchain controller can delete the personal data

identifiers at the data subject's request. Once the identifiers are erased, the GDPR protocol treats it as anonymized data. At this point, the pseudonymization is irreversible and the controller is no longer obligated to comply with GDPR requirements.

## 3.2 National Legislation

### *3.2.1 Spain*

Protection of individuals with regard to the processing of personal data is a fundamental right protected by Article 18.4 of the Spanish Constitution. A document of consolidated Spanish legislation on data protection, personal security and digital rights (Law 3/2018) can be found at https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf. The Act consists of ninety-seven articles structured in ten titles, twenty additional provisions, six transitory provisions, one repeal provision and sixteen final provisions. The supervisory data protection authority of Spain can be reached at https://www.aepd.es/es, where practical information on data protection rights and obligations, as well as answers to frequent questions are provided.

### *3.2.2 Switzerland*

The Swiss Federal Act on Data Protection of 19 June 1992 aims to protect the privacy and the fundamental rights of persons when their data is processed (https://www.admin.ch/opc/en/classified-compilation/19920153/index.html). It applies to the processing of data pertaining to natural persons and legal persons by:

a. Private persons;
b. Federal bodies.

Additionally, the Federal Act on Data Protection has as its central goal (a) the maintenance of good data file practice and (b) the facilitation of international data exchange by providing a comparable level of protection. To accomplish the latter goal, it regulates the transborder transfer of data in those cases when there is a need for the protection of privacy. Transfers may be prohibited if, for example, the recipient's country cannot provide an adequate level of data protection. Both, private individuals and federal bodies who may be involved in cross-border data disclosure, are subject to the duty of due care. The transfer of data files abroad has to be notified in case of a lack of adequate protection. In the absence of such protection, data may only be disclosed abroad if other safeguards, in particular contractual clauses or rules within the same legal person, guarantee protection.

The national supervisory data protection authority in Switzerland is the Federal Data Protection and Information Commissioner (https://www.edoeb.admin.ch/edoeb/en/home.html), which is appointed by the Federal Council and supervises the compliance of Federal authorities with the Federal Act on Data Protection.

### *3.2.3 Greece*

The national supervisory data protection authority in Greece is the Hellenic Data Protection Authority (https://www.dpa.gr). Data protection law grants the data subjects, i.e. individuals, certain rights and imposes certain responsibilities on data controllers, i.e. anyone who keeps personal data in a file and processes it.

Apart from the GDPR and the EU directive 2016/680, the most recent national laws are the following:

Law 4624/2019 - Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 and other provisions.

Law 3471/2006 - Protection of personal data and privacy in the electronic telecommunications sector and amendment of law 2472/1997.

### *3.2.4 Sweden*

The Swedish Data Protection Authority (https://www.datainspektionen.se/) is a public authority with the goal to protect the individual's privacy in the information society. It works to prevent encroachment upon privacy through information and by issuing directives and codes of statuses.

In Sweden, the national regulation is called SFS 2018: 218 Law, also known as Data Protection Act, and provides supplementary provisions to the EU Data Protection Regulation. The Data Protection Act is subsidiary in relation to deviating provisions of another law or regulation that regulates the processing of personal data. This means that the provisions of the law should not be applied if there are deviating provisions in other laws.

## 3.3 Smart Grid Task Force Guidelines

Data security and privacy guidelines have been provided by various organizations and working groups, such as Smart Grid Task Force (SGTF). Several reports were studied in order to identify the guidelines relevant to the PARITY system and LEM/LFM implementation.

In report document [12], SGTF provides recommendations to guarantee privacy and network security for smart-metering systems. In this report was proposed a Network Code on Cybersecurity, which aims to tackle existing cybersecurity risks and protect from future threats. Privacy and Security in integrated networks is a continuous effort from all stakeholders in order to achieve a strong energy structure. The base for the recommended practices is the idea to handle cybersecurity in a universal and risk-based method. The recommendations proposed by the Network Code on cybersecurity can be divided into three major sections [12]. The Baseline Cybersecurity block is a baseline applicable to all operators, bearing in mind their distinct capabilities and capacities. The Advanced Cybersecurity actions are especially for operators of essential services, the ones identified as vital for the economy's operation. The Supportive Elements are tools to endorse security protocols implementation.

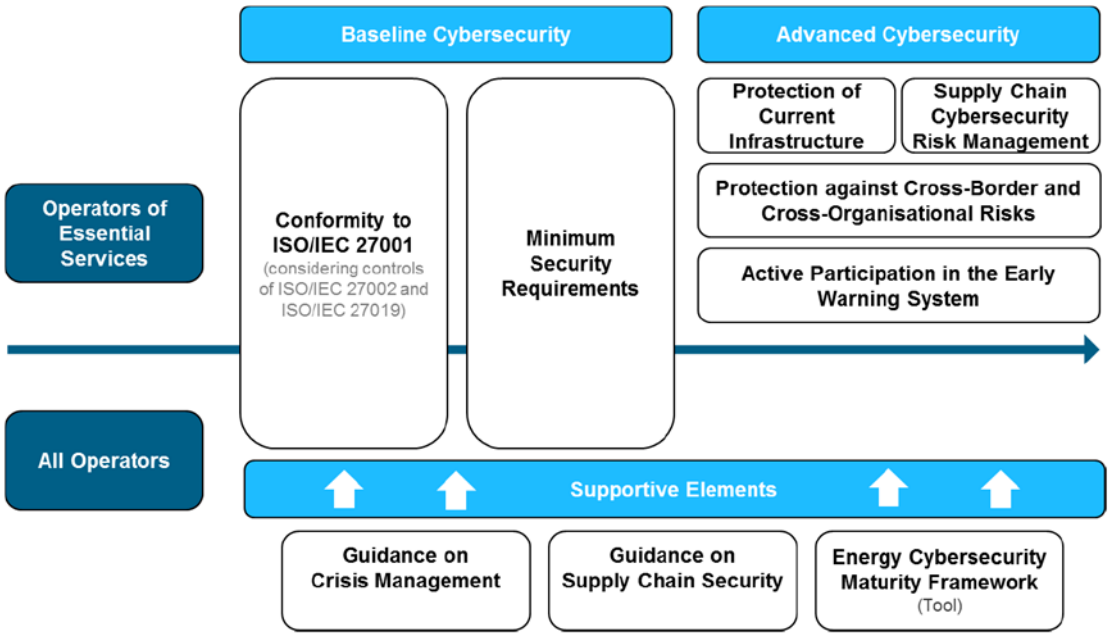



**Figure 2. Recommended Structure for the Network Code on Cybersecurity [12].**

A minimum security level is required for specific components of the energy system. The EU Cybersecurity Act defines minimum cybersecurity requirements, and those can be converted into international standards. These minimum security requirements are crucial for the protection of the EU Energy system. An indicative non-exhaustive list is provided in Table 1.

**Table 1. Minimum security requirements per area.**

| Area | Requirements |
|---|---|
| **Communication** | Use the international IEC 62351 standard series for communication protocols |
| **Categorization** | Split object into domains of:<br>• OT products: RTU, Protection Relay, Industrial Router, Smart Meter…<br>• OT systems: Control Centre, Primary Substation, Asset-Monitoring, Smart Metering, Micro-Grid, Industrial Router…<br>• IT Services: Cloud (on-/off-premise), Network Management (e.g. fault- , configuration-, performance management)… |
| **Methodology** | Use a methodology based on ISO/IEC 27005:2018<br>• Identify and assess countermeasures.<br>• Re-assess likelihood of occurrence and impact.<br>• Define residual risks.<br>• Compare it with passable risks.<br>• Identify additional cybersecurity measure. |
| **Methodology - Context establishment** | System outline.<br>• Classification of products, systems and services.<br>• Risk-impact matrix.<br>• EU level protection reference architecture should consider architectures presented by international standards. ENTSO-E and EU-DSO should align on respective architecture. |
| **Methodology - Risk Treatment** | Review of risks should be performed by an expert group formed by relevant stakeholders. |
| | International standards recommended:<br>• OT products: IEC 62443-4-1/-4-2<br>• OT systems: IEC 62443-2-4/-3-3<br>• IT Services: Domain specific → Verify it with ENISA. |
| | Document residual risks |

ENISA SGTF EG2 provides a proposal for a list of security measures for smart grids in [13]. Moreover, baseline requirements on cyber security for consumer Internet of Things are provided by the ETSI EU standard and described in [14]. The recommendations from ENISA and ETSI were assessed according to the relevance for PARITY, and were prioritized. The list is provided in Table 2. It should be noted that "Corporate" indication means that the requirement is important for an organisation applying the PARITY solution, but not during system development stage.

**Table 2. ENISA and ETSI recommendations.**

| Measure | Description | Priority |
|---|---|---|
| **No universal default passwords** | All consumer IoT device passwords shall be unique per device or defined by the user. | High |
| | Passwords shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device | High |
| | Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage. | High |
| | Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used. | High |
| | When the device is not a constrained device, it shall have a mechanism available, which makes brute-force attacks on authentication mechanisms via network interfaces impracticable. | High |
| **Implement a means to manage reports of vulnerabilities** | The manufacturer shall make a vulnerability disclosure policy publicly available | Corporate |
| | Disclosed vulnerabilities should be acted on in a timely manner | Corporate |
| | Manufacturers should continually monitor for, identify and rectify security vulnerabilities | Corporate |
| **Keep software updated** | All software components in consumer IoT devices should be securely updateable. | High |
| | When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates. | High |
| | An update shall be simple for the user to apply | High |
| | Automatic mechanisms should be used for software updates | High |
| | The device should check after initialization, and then periodically, whether security updates are available. | High |
| | If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications. | High |
| | The device shall use best practice cryptography to facilitate secure update mechanisms | High |
| | Security updates shall be timely. | High |

| | | |
|---|---|---|
| | The device should verify the authenticity and integrity of software updates. | High |
| | Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship. | High |
| | The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update. | High |
| | The device should notify the user when the application of a software update will disrupt the basic functioning of the device. | High |
| | The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period. | Corporate |
| | For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user. | Low |
| | For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable | Low |
| | A Continuous Deployment and Continuous Integration test bed should be deployed and all sub-systems should be regularly checked against it (including security and reliability test) | High |
| | The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface. | High |
| **Securely store sensitive security parameter** | Sensitive security parameters in persistent storage shall be stored securely by the device | High |
| | Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software | High |
| | A comprehensive logging system should be included in the solution including access and modification logs | High |
| | The logging system should be signed to ensure that no modification has been carried out (for example storing the log in the blockchain solution) | High |
| | Users' accounts with different permits should be created for each components. The logging system | High |

| | | |
|---|---|---|
| | should be secure on both OTA and physical connections | |
| | Hard-coded critical security parameters in device software source code shall not be used | High |
| | Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices. | High |
| **Communicate securely** | The consumer IoT device shall use best practice cryptography to communicate securely | High |
| | The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography. | High |
| | Cryptographic algorithms and primitives should be updateable. | High |
| | Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface. | High |
| | Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. | High |
| | Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage. | High |
| | The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces. | High |
| | The manufacturer shall follow secure management processes for critical security parameters that relate to the device. | Corporate |
| **Minimize exposed attack surface** | All unused network and logical interfaces shall be disabled. | High |
| | In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information. | High |
| | Device hardware should not unnecessarily expose physical interfaces to attack | High |
| | Where a debug interface is physically accessible, it shall be disabled in software. | High |

| | | |
|---|---|---|
| | The manufacturer should only enable software services that are used or required for the intended use or operation of the device. | High |
| | Code should be minimized to the functionality necessary for the service/device to operate. | High |
| | Software should run with least necessary privileges, taking account of both security and functionality. | High |
| | The device should include a hardware-level access control mechanism for memory | High |
| | The manufacturer should follow secure development processes for software deployed on the device. | Corporate |
| **Ensure software integrity** | The consumer IoT device should verify its software using secure boot mechanisms. | High |
| | If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function. | High |
| **Ensure that personal data is secure** | The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography. | High |
| | The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage. | High |
| | All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user | High |
| **Make systems resilient to outages** | Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power. | High |
| | Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power. | High |
| | The different solutions should be able to answer to authenticated Magic SysRq actions both OTA and physically | Low |
| | The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration. | High |
| **Examine system telemetry data** | If telemetry data is collected from consumer IoT devices and services, such as usage and | High |

| | | |
|---|---|---|
| | measurement data, it should be examined for security anomalies. | |
| **Make it easy for users to delete user data** | The user shall be provided with functionality such that user data can be erased from the device in a simple manner. | High |
| | The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner. | High |
| | Users should be given clear instructions on how to delete their personal data. | High |
| | Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications. | High |
| **Make installation and maintenance of devices easy** | Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability. | Medium / Highly desirable |
| | Preventive/corrective physical maintenance should be carried out regularly. | Medium / Highly desirable |
| | An inventory component should be developed or used in the solution. | Medium / Highly desirable |
| | The manufacturer should provide users with guidance on how to securely set up their device. | Medium / Highly desirable |
| | The manufacturer should provide users with guidance on how to check whether their device is securely set up. | Medium / Highly desirable |
| **Validate input data** | The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices. | High |
| **Data protection provisions for consumer IoT** | The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers | High |
| | Reused device or services have to ensure that no personal data is revealed | High |
| | Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way. | High |
| | Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time. | High |
| | If telemetry data is collected from consumer IoT devices and services, the processing of personal data | High |

| | | |
|---|---|---|
| | should be kept to the minimum necessary for the intended functionality. | |
| | If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes. | High |

USEF provides a privacy and security guideline [7] that is structured around nine "windows" on privacy and security aspects in smart energy systems. These are presented in Table 3. The guideline forms the basis for the logical security architecture that is part of the Information and Communication Technologies framework.

**Table 3. Windows on privacy & security in smart energy systems.**

| | Title | Description |
|---|---|---|
| **1** | Privacy-value creation trade-offs | Individuals and business can both benefit from sharing certain privacy sensitive data. It might allow for tailor made propositions to the end-user or more efficient management of the energy system. How do we accommodate all legitimate interests and objectives? |
| **2** | Data management | Data management includes, among others, the collection, storing, processing and mining of data. What data are collected and for which purpose? How long are the data retained and why? When should it be possible to trace data back to its origin? Who owns what data? |
| **3** | Data communication | Smart energy systems will generate a lot of data that needs to be transported over an infrastructure to the point(s) where they are used. What is the desired security level for different types of data communication? |
| **4** | Confidentiality | Confidentiality refers to limiting information access and disclosure to authorized resources and preventing access by or disclosure to unauthorized resources. The consequences of a breach are different for the different stakeholders (loss of privacy for a Prosumer, loss of goodwill, competitive disadvantage for a retailer). What are necessary and acceptable levels of confidentiality for the different parts of the system? |
| **5** | Integrity | Integrity means that data cannot be modified undetectably. Where in the smart energy system is integrity more important than availability, or more important than confidentiality? |
| **6** | Availability | Availability refers to the availability of information resources including systems, processes and data elements. What are necessary and acceptable levels of availability for the different components of a smart energy system? |
| **7** | Disaster Recovery | No (security) system is perfect. What needs to be done in the case of unforeseen situations? How to mitigate the |

| | | |
|---|---|---|
| | | fall-out from a security/privacy breach? How are responsibilities divided between parties? |
| **8** | Identification, Authentication, Authorization | Identification is the process of showing who you are. The identification is validated through the process of authentication, which verifies that you are who you say you are. Authorization is the process of verifying that "you are permitted to do what you are trying to do." |
| **9** | Risk assessment | Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat. |

# 4. PILOTS SECURITY AND PRIVACY REQUIREMENTS

DPIA was conducted in order to identify important privacy and security risks as well as additional related requirements that shall be taken into account. All pilot partners filled in the DPIA document, including CERTH and HYPERTECH as they host pre-pilot setups for testing the PARITY solutions. The DPIA document template that was distributed was created especially for the PARITY project based on the DPIA templates [8] and [9]. The former is related to GDPR guidelines, while the latter, proposed by the Smart Grid Task Force, targets Smart Grid and Smart Metering systems.

The DPIA document template is organized into eight sections. The first one, which is the introduction, analyses the purpose of the document, highlighting that it ensures GDPR compliance. PARITY objectives are mentioned and the type of data, necessary for the project execution, is defined. The second section describes how proper data collection, transfer, storage and sharing are going to be achieved. Data will be anonymized and user rights will be protected. The third section, consultation process, ensures that project's Ethical Advisory Board will address any ethical and legal issues that may arise, including privacy issues related to data collection. Necessity and proportionality concerns are analysed in section 4. It is mentioned that data will be stored only if this is absolutely necessary. Data quality will be assured, performing the essential pre-processing/cleaning and data minimization will be achieved by periodically reviewing the stored data. Section 5, risk identification and assessment, introduces a list of possible privacy and security risks that are evaluated with regard to their likelihood and severity of harm. To this end, 5 different levels (1: Negligible – 5: Maximum) have been defined. Then, the overall priority for each risk can be determined within the range 1 to 4 (1: Red – 4: Green). Section 6, namely measures identification, describes all the measures that can be taken in order to reduce or eliminate the risks previously identified with overall priority up to 3. It is noted that the measures must be GDPR-compliant. Section 7 provides a checklist of GDPR provisions, and finally, the last section records the outcomes.

After the interpretation of the DPIA results, important privacy and security risk categories affecting all or most of the pilots were identified (Table 4). These risks are related to GDPR referring especially to the processing of personal data, and the data subject's rights with regard to data manipulation (e.g. deletion of data). Failures and malfunctions of devices or systems was another important risk category as well as internet and network problems that can affect accessibility and the data collection process. Lastly, risks related to abuse, such as unauthorized activities, malicious activities and compromising confidential information, have been identified as high priority.

Medium and high security and privacy risks identified per each pilot through the DPIA were collected. These led to the definition of the respective requirements that must be considered by the partners during the design and implementation of the PARITY system. For each privacy/security requirement, measures that should be applied were proposed by the pilot partners in the DPIA. The measures can be divided into three categories, which are the following: (1) Regulations, procedures & contracts, (2) Infrastructure-hardware installation, (3) Software, data exchange and storage.

**Table 4. Privacy and security risk levels per pilot site.**

| Risk description | Spanish Pilot | Swiss pilot | Greek pilot | Swedish pilot |
|---|---|---|---|---|
| **Illegitimate processing of Personal Data** | | | | |
| No lawfulness of processing | High | High | High | High |
| Collection exceeding purpose | High | - | Medium | - |
| Unclear responsibilities for Data Processing | High | - | High | - |

| | | | | |
|---|---|---|---|---|
| The protection of data is compromised outside the European Economic Area (EEA) | High | High | High | - |
| **Inadequate information of the data subject** | | | | |
| Incomplete information | High | High | High | - |
| **Violation of the data subject's rights** | | | | |
| Inability to execute individual rights (inspection rights) | High | High | High | High |
| Prevention of objections | High | High | High | High |
| A lack of transparency for automated individual decisions | Medium | High | Medium | Medium |
| Lack of correction of Personal Data | Maximum | - | High | High |
| Lack of erasure of Personal Data | Maximum | - | Maximum | - |
| **Compliance violations in the contracts** | | | | |
| Missing or incorrect contractual Data Protection clause | High | - | High | - |
| **Personal Data integrity loss** | | | | |
| Lack of quality of data for the purpose of use | High | High | High | Medium |
| Inability to respond to requests for subject access, correction or deletion of data in a timely and satisfying manner | High | High | High | High |
| **Damage to individual** | | | | |
| Discrimination | High | High | High | - |
| Identify Theft or Fraud | High | High | High | High |
| Financial loss | High | High | High | Medium |
| Other significant economic or social disadvantage | High | - | High | - |
| **Physical attack (deliberate/ intentional)** | | | | |
| Fraud | High | High | High | - |
| Sabotage | High | High | High | - |
| Vandalism | High | High | High | - |
| Theft (of devices, storage media and documents) | High | High | High | - |
| Information leak /sharing | High | High | High | High |
| Unauthorized physical access / Unauthorized entry to premises | High | High | High | Medium |
| Coercion, extortion or corruption | High | High | High | - |
| Damage from the warfare | High | - | High | - |
| Terrorist attack | High | - | High | High |
| **Unintentional damage / loss of information or IT assets** | | | | |
| Information leak /sharing due to human error | High | High | High | Maximum |
| Erroneous use or administration of devices and systems | High | High | High | High |

| | | | | |
|---|---|---|---|---|
| Unintentional change of data in an information system | High | High | High | High |
| Inadequate design and planning or improper adaptation | High | High | High | High |
| Loss of (integrity of) sensitive information | Maximum | High | Maximum | Maximum |
| **Disaster (natural, environmental)** | | | | |
| Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy winds, fire, water etc.) | High | - | High | - |
| **Failures/ Malfunction** | | | | |
| Failure of devices or systems | High | High | High | - |
| Failure or disruption of communication links (communication networks) | Maximum | High | High | Medium |
| Failure or disruption of main supply | Maximum | High | High | - |
| Malfunction of equipment (devices or systems) | High | High | High | - |
| **Outages** | | | | |
| Absence of personnel | High | Maximum | High | - |
| Loss of support services | High | High | High | - |
| Internet or Network outage | Maximum | High | Maximum | - |
| **Eavesdropping/ Interception/ Hijacking** | | | | |
| Interception of information | - | - | High | High |
| Interfering radiation | High | High | High | - |
| Replay of messages | - | High | High | High |
| Man in the middle / Session hijacking | - | High | - | High |
| **Nefarious Activity / Abuse** | | | | |
| Identity theft (Identity Fraud/ Account) | High | High | High | High |
| Denial of service | High | High | High | - |
| Malicious code/ software/ activity | High | High | High | High |
| Manipulation of hardware and software | High | High | High | High |
| Misuse of information/ information systems | High | High | High | - |
| Unauthorized activities | High | High | High | High |
| Compromising confidential information | High | High | High | High |
| Abuse of authorizations | High | High | High | - |

## 4.1 Security Requirements

Critical security requirements as derived from the DPIA (highest risk level) per each pilot site are presented next. Moreover, the majority of the risks were characterized with ‘High’ priority level as already shown, so these were also considered.

#### *4.1.1 Spanish pilot*

It is critical for the Spanish pilot to implement measures to protect from failures of communication links and main supply. Moreover, it was indicated that the system has to be able to recover automatically from internet or network outage.

#### *4.1.2 Swiss pilot*

Availability of personnel is reported as critical for the Swiss pilot. However, this requirement is not related to the system's specifications.

#### *4.1.3 Greek pilot*

It is critical for the Greek pilot site that the system is able to recover automatically from internet or network outage.

#### *4.1.4 Swedish pilot*

No critical security requirements were reported for the Swedish pilot, however, several risks were marked as of high priority.

### 4.2 Privacy Requirements

Critical privacy requirements as derived from the DPIA (highest risk level) per each pilot site are presented next.

#### *4.2.1 Spanish pilot*

A critical privacy requirement by the Spanish pilot is to respect data subject's rights, especially the correction and erasure of personal data. Moreover, protection of sensitive information from unintentional loss is another critical requirement.

#### *4.2.2 Swiss pilot*

No critical privacy requirements were reported for the Swiss pilot, however, several risks were marked as of high priority.

#### *4.2.3 Greek pilot*

Two critical privacy requirements were indicated by the Greek pilot: (1) to provide the right to erase personal data on user's request and (2) to protect integrity of sensitive information.

#### *4.2.4 Swedish pilot*

For the Swedish pilot, the two most important privacy requirements are the prevention of improper information sharing and the protection of sensitive information from unintentional loss.

## 4.3 Privacy and Security Measures

The measures that shall be taken in order to meet the security and privacy requirements derived from the DPIA are described in section 5 and section 6, respectively. A summary is provided for reference in Table 5 below.

**Table 5. Privacy and security measures.**

| Privacy Measure | Category |
|---|---|
| Managing contracts between Data Controllers and Data Processors | Regulations, procedures & contracts |
| Anonymizing personal data (or use pseudonyms) | Regulations, procedures & contracts |
| Permit the exercise of the right to object (to the use of personal data) | Regulations, procedures & contracts |
| Limits on the use of information for specific purpose | Regulations, procedures & contracts |
| Provide the individual control over his/her data e.g. through a secured portal | Regulations, procedures & contracts |
| Sign contracts with the customer of the pilot site | Regulations, procedures & contracts |
| Create contracts with third parties for the same services | Regulations, procedures & contracts |
| Create contracts that respect the law, audits and updates | Regulations, procedures & contracts |
| Grant access to the systems only to specific trained personnel | Regulations, procedures & contracts |
| Create detailed, comprehensive contracts with sufficient information for the subject | Regulations, procedures & contracts |
| Translate all information from English into customer language | Regulations, procedures & contracts |
| Creation of consent forms | Regulations, procedures & contracts |

| | |
|---|---|
| Manage personal data violations | Regulations, procedures & contracts |
| Design and implement a complaints-handling system | Regulations, procedures & contracts |
| In the context of living lab, make presentations to the users about purpose and collection and use of data | Regulations, procedures & contracts |
| Manage third parties with legitimate access to Personal Data | Regulations, procedures & contracts |
| **Security Measure** | **Category** |
| Encrypting personal data | Software, data exchange and storage |
| Restrict access to Internet and uncontrolled private networks | Software, data exchange and storage |
| Reduce software vulnerabilities by providing updates (automated updates to clients) | Software, data exchange and storage |
| Reduce hardware vulnerabilities (frequent monitoring, UPS connection, technical support) | Infrastructure-hardware installation |
| Communications networks: Use of security protocols | Software, data exchange and storage |
| Monitor the integrity of personal data | Software, data exchange and storage |
| Implement automated controls on the data quality (algorithmic reconstruction of missing data) | Software, data exchange and storage |
| Perform maintenance, remote surveillance and keep data backups | Software, data exchange and storage |
| Logging the activity on the IT system and provide automated monitoring | Software, data exchange and storage |
| Protection of personal data archives | Software, data exchange and storage |
| Ensure data plausibility by cross-checking | Software, data exchange and storage |

| | |
|---|---|
| Ensure anti-hacking protection of IT systems | Software, data exchange and storage |
| Combat malicious codes | Software, data exchange and storage |
| Reduce the vulnerabilities related to the circulation of paper documents | Software, data exchange and storage |
| Monitor logical access controls | Software, data exchange and storage |
| Destruction schedules for personal information | Software, data exchange and storage |
| Minimize personal data retention | Software, data exchange and storage |
| Reduce the vulnerabilities of individuals | Software, data exchange and storage |
| Audit, verification with external tests | Software, data exchange and storage |

# 5. PARITY SECURITY ACCESS CONTROL FRAMEWORK

This section describes the security access control framework, which has been formulated by integrating the measures for data security that will be implemented to the PARITY system.

## 5.1 Role-based Access Control

Role Based Access Control (RBAC) is a common approach to managing users' access to resources or operations. Permissions specify exactly which resources and actions can be accessed. The basic principle is that instead of separately managing the permissions of each user, permissions are given to roles, which are then assigned to users, or group of users.

In PARITY, all the components will use the security access control framework in order to regulate the information that each module is allowed to access. This way, the components only have access to the data they actually need, making easier to control and minimize the changes of a fraudulent use of the information.

## 5.2 Authentication

Authentication is the process of identifying users that request access to a system, network, or device. The PARITY components such as Demand Flexibility Profiling and Human-Centric Power2Heat, Information Management Layer Cloud and IoT Gateway (including also the integration with the blockchain platform) are designed to use the OAuth2 industry-standard protocol combining also JSON WebTokens (JWT) in order to meet the authentication expectations that will be addressed by the security access control framework.

OAuth (Open Authorization) is a standard framework that allows login access to third-party websites and applications without exposing user account credentials and information. In the traditional client-server authentication models, the client requests an access-restricted resource (protected resource) on the server by authenticating with the server using the resource owner's credentials. In order to provide third-party applications access to restricted resources, the resource owner shares its credentials with the third party. However, this creates several problems and limitations:

- Third-party applications are required to store the resource owner's credentials for future use, typically a password in clear-text
- Servers are required to support password authentication, despite the security weaknesses inherent in passwords
- Third-party applications gain overly broad access to the resource owner's protected resources, leaving resource owners without any ability to restrict duration or access to a limited subset of resources
- Resource owners cannot revoke access to an individual third party without revoking access to all third parties, and must do so by changing the third party's password
- Compromise of any third-party application results in compromise of the end-user's password and all of the data protected by that password

OAuth addresses these issues by introducing an authorization layer and separating the role of the client from that of the resource owner. In OAuth, the client requests access to resources controlled by the resource owner and hosted by the resource server, and is issued to a different set of credentials than those of the resource owner. Instead of using the resource owner's credentials to access protected resources, the client obtains an access token - a string denoting a specific scope, lifetime, and other access attributes. Access tokens are issued to third-party clients by an authorization server with the approval of the resource owner. The client uses the access token to access the protected resources hosted by the resource server.

OAuth2 is the latest version of that standard. It defines the authorization flows between clients and one or more services in order to gain access to protected resources.

JSON Web Token, or JWT, is a specification for the representation of claims to be transferred between two parties. The claims are encoded as a JSON object used as the payload of an encrypted structure, enabling the claims to be digitally signed or encrypted. JWT can be chosen as the format for access and refresh tokens used inside the OAuth2 protocol.

## 5.3 Authorization

Authorization is the process of specifying access rights/privileges to a user, system, or device. OAuth2 defines four main roles that facilitate the procedure of separating the role of the client from that of the resource owner. These roles are:

- Resource Owner, refers to an entity capable of granting access to a protected resource. In case the resource owner is a person then it is referred to an end-user.
- Client, defines an application that making protected resource requests on behalf of the resource owner using Resource Owner authorization.
- Resource Server, is the server which is hosting the protected resources. It is capable of accepting protected resource request using access tokens.
- Authorization Server, refers to the server which issue access tokens to the client after successfully authenticating the resource owner and obtaining authorization.

The following Abstract Protocol Flow reveals on how the above roles interact with each other:

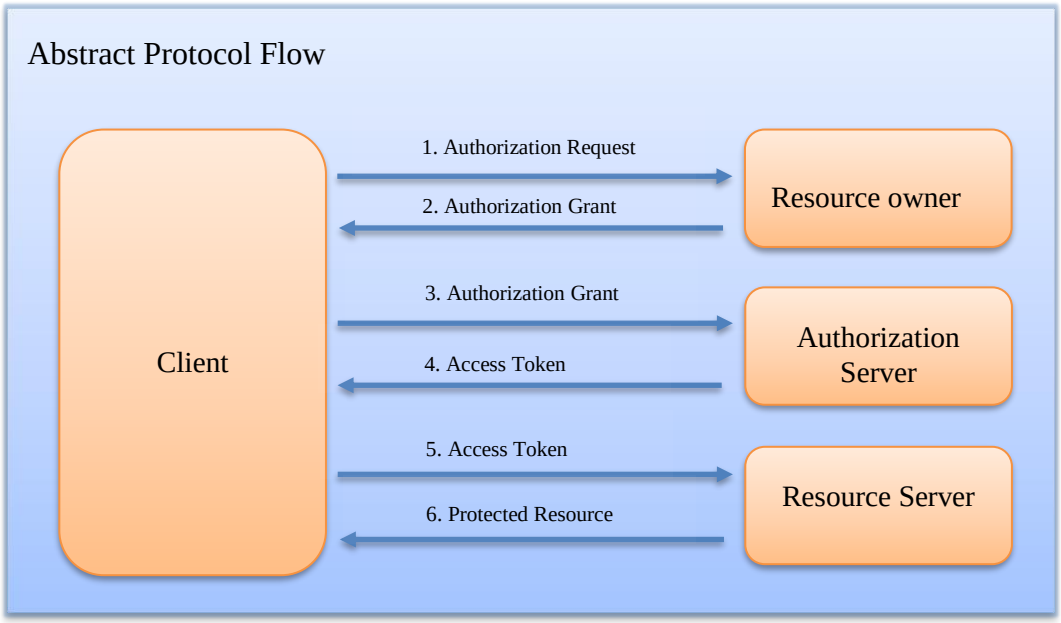



**Figure 3. OAuth2 process flow.**

In a nutshell, the OAuth2 flow, illustrated also in Figure 3, describes the interaction between the four roles and includes the following steps:

1. The *client* requests authorization to access service resources from the *resource owner*.
2. If the *resource owner* authorized the request, the *client* receives an authorization grant.

3. The *client* requests an access token from the *authorization server* by presenting authentication of its own identity, and the authorization grant.
4. If the client identity is authenticated and the authorization grant is valid, the *authorization server* issues an access token to the client. Authorization is complete.
5. The *client* requests the resource from the *resource server* and presents the access token for authentication.
6. If the access token is valid, the *resource server* serves the resource to the *client.*

In the above aforementioned figure, the first four steps obtaining an **authorization grant** and an **access token** (& refresh token). The *authorization grant* type depends on the method used by the client to request authorization. OAuth2 defines four grant types, each of which is useful in different cases:

1. Authorization Code, used with server-side applications
2. Implicit, used with Mobile or Web applications
3. Resource Owner Password Credential, used with trusted Applications, such as those owned by the service itself
4. Client Credential, used to access its own protected resources

The PARITY components of Demand Flexibility Profiling and Human-Centric Power2Heat, Information Management Layer Cloud and IoT Gateway are designed to use both Authorization Code and Implicit grant types.

*Access tokens* are credentials used to access protected resources. An access token is a string representing an authorization issued to the client. Tokens have specific duration of access, which are granted by the resource owner. In principle, access tokens provide an abstraction layer, replacing different authorization methods (i.e. username/password) with a single token understood by the resource server, removing the need from the resource server to understand a wide range of authentication method. During PARITY project is proposed to be used JSON Web Token access tokens for authorization between components.

*Refresh tokens* carry the information necessary to get a new access token. In other words, whenever an access token is required to access a specific resource, a client may use a refresh token to get a new access token issued by the authentication server. Common use cases include getting new access tokens after old ones have expired, or getting access to a new resource for the first time. Refresh tokens can also expire but are rather long-lived. Refresh tokens are usually subject to strict storage requirements to ensure they are not leaked. They can also be blacklisted by the authorization server.

## 5.4 Secure Protocols

The security protocol that PARITY components will use for their intercommunication will be based on the Transport Layer Security (TLS). TLS aims both at data privacy and at integrity using reliable and stable messages transmission during connections, preventing undetected loss of data.

Every PARITY component should be able to implement TLS configurations in order to be aligned with security protocol requirements.

In order to enhance security also in the authorization framework (OAuth2 & JWT), best practices should be followed during the design and the implementation:

- *Secret & Safe Access Tokens*, the signing key should be treated like any other credential and revealed only to services that need it.
- *Token expiration*, once a token is signed, it is valid forever, unless the signing key is changed or expiration explicitly set.

- *Embrace TLS*, tokens should not be sent over non - HTTPS connections.
- *Not including sensitive data to the token payload.*

## 5.5 X.509 Public Key Certificates

X.509 is a standard defining the format of public key certificates. These certificates are used in various protocols, such as TLS/SSL, as well as in electronic signatures. An X.509 certificate contains a public key and an identity, and can be self-signed or signed by a certificate authority (CA). It can be used to verify that a public key belongs to the user, computer or service identity contained within the certificate.

Certificate based authentication allows clients (users or applications) to securely access a server by exchanging a digital certificate instead of a username and password. This means that the client is not sending a username or password to the server, which helps to prevent some types of attacks. Certificate based authentication is built by leveraging the X.509 public key infrastructure standard. The client has to use a valid X.509 certificate that is generated and signed by the same root certificate authority as the server. The use of certificates by PARITY components is planned to verify the identity of critical components that act as servers.

## 5.6 Data Encryption

Data encryption is a security method, which encodes data in a way that a correct key is required in order to access/decrypt them. Encrypted data appear scrabbled or unreadable to a person or machine accessing them without permission. There are two types of data with regard to their state: data in motion and data at rest. Data in motion, also referred as “active data”, are used in the context of being in a database or being processed by an application. Data at rest are “inactive data” that are stored physically in any digital form, such as databases, off-site backups, etc. The encryption of data in motion within PARITY will be implemented when exchanging data among components using the security protocols already mentioned. The encryption of data at rest is a key protection against a data breach, and should only employ strong encryption methods such as AES or RSA. Even though encryption is not mandatory for being compliant with GDPR, it is a proposed measure. Within PARITY, full database encryption at rest will be enabled where possible, also depending on the support by the DBMS, since this feature may only be available in Enterprise DB editions.

Another related functionality that will be applied by the common repository of the system is user password hashing. Hashing is a one-way mechanism that maps data of any size to a fixed-size bit string using a hash function (e.g. SHA-256). After applying the hash function, a plain password has been turned into a scrambled representation, derived from the combination of both the password and a key. This operation is not reversible.

## 5.7 Security Breach Response Plan

In order to minimize the impact and deal with an attack or security breach, a response plan will be applied. A first measure is to conduct regular backups of the databases that will be stored offline. Moreover, specific people (e.g. DPOs at pilot sites, PARITY partners) will be assigned to be responsible for responding to such incidents. Based on the severity of the security issue, external support may be requested (e.g. for forensics recovery). Lastly, in any case, technology development partners will have to examine the issue in order to proceed to the proper updates and actions to solve any security vulnerabilities.

# 6. PARITY PRIVACY SPECIFICATIONS

## 6.1 Anonymization

IoT Gateway, a multiprotocol gateway that will streamline the information flow between the physical world and PARITY framework, constitutes a powerful sensor fusion responsible for gathering ambient and environmental conditions, occupancy patterns as well as control and comfort preferences. All the data that are gathered by the IoT Gateway will be anonymized and will confront with the output of the Data Protection Impact Assessment (DPIA).

## 6.2 Pseudonymization

After evaluating all the options available for blockchains to achieve GDPR compliance, pseudonymization offers the most effective solution. This approach enables the blockchain to meet the GDPR data privacy requirements without losing any of its operational advantages.

Pseudonymization provides an ideal middle ground between the GDPR requirements and blockchain features. The maintenance of personal identifiers off the chain allows the blockchain to process information without infringing the data subject's privacy rights. In this way, blockchain permanence, immutability, decentralization and distribution only enhance the data subject's safety. As such, pseudonymization offers the data subject the best of both worlds.

However, the blockchain still needs to apply the pseudonymization procedures in compliance with GDPR requirements. This means that the blockchain controller should apply stringent data privacy controls on the personal data maintained off the chain. This is necessary until the personal data is safely erased.

### *6.2.1 Pseudonymization governance framework*

Blockchain data privacy through pseudonymization depends on the careful administration of GDPR protocols. This can be achieved by developing a strong pseudonymization governance framework for the blockchain controller. This framework should be established in compliance with the GDPR policy and applied to all personal data collected by the controller. A reliable pseudonymization framework should be fully demonstrable and auditable. Below are some of the main elements that should feature in this governance framework.

*Definition of Personal vs Non-Personal Data*: The first step of ensuring proper governance of the pseudonymization framework is to determine what constitutes personal data. Identifying the types of data can be stored on the blockchain without violating GDPR policy is vital to achieving and maintaining compliance. This element of compliance requires businesses to control how and why data is collected before it is committed to the blockchain. Businesses should employ screening protocols to prevent personal data from being added to the blockchain. Accidentally holding or processing unprotected personal data on the blockchain is also considered to be a violation of GDPR policy. This is a likely occurrence when data subjects are working with application programming interfaces (API) that interact with the blockchain.

*Control of Access to Pseudonymization links*: One of the most sensitive aspects of data privacy is controlling who has access to personal data. In this model, personal data is masked by assigning pseudonyms to its personal identifiers off the blockchain. As such, whoever has access to the pseudonymized links can attribute them to identifiable persons. This is why controlling access to these links on the blockchain is vital. Without strictly controlling the accessibility of the pseudonymized data, GDPR compliance cannot be achieved.

*Logical Erasure of Pseudonymization links*: The final stage of GDPR compliance is achieved when the links between the blockchain and personal identifiers off the chain are deleted. When this deletion is intentional, it is referred to as the logical erasure of personal data. Deletion of personal identifiers anonymizes the personal data on the blockchain. The GDPR requires blockchain architects to ensure that the data subjects cannot be re-identified once the pseudonymization links have been erased. The GDPR policy does not have any restrictions on how fully anonymized data is managed on the blockchain.

## 6.3 Data Aggregation

Data aggregation technique will be applied in order to present information only in groups and not per individual, towards enhancing privacy. In particular, aggregated flexibility data will be presented to the user of the Aggregator Toolset.

## 6.4 Data Handling and Sharing

As far as data handling is concerned, the right to erasure will be supported where possible, as it is a GDPR requirement. The process will be initiated by a Prosumer user who will make a request through the UI. Moreover, a user will be able to make a request to unregister from the LEM/LFM.

Regarding data sharing through human intervention, contracts between data controllers and data processors will specify exactly how the data will be used, the responsible persons, and the objective of processing. Files containing data e.g. measurements for analysis and verification, will be extracted and provided to data processor as password-protected archives.

# 7. PARITY SYSTEM SECURITY IMPLEMENTATION

This section describes the implementation of security measures by the main components of the PARITY system. The overall system architecture, descriptions and specifications of the components are presented in the confidential deliverable *D3.5 PARITY System Architecture*.

## 7.1 PARITY IoT Network

The IoT Network that will be provided in order to cover all the technical and technological objectives of PARITY project is formulated by physical (hardware) as well as software components. In the first category are included the IoT Gateway, the on-board sensors and all the off-the-shelf equipment needed for data acquisition, real-time monitoring and actuating while these components comprise the main Wireless Sensor Network (WSN) of the project. In the second category (software components) are included components like PARITY Oracle (that is presented in section 7.3) and IML Cloud. The IML Cloud constitutes the component with the main responsibility to collect and process all the data acquired through the sensing equipment and is related to building information having strong interaction with flexibility-relevant software components like Demand Flexibility and Human-Centric P2H component and the common repository that will be developed in the PARITY project (LEM/LFM Repository) . In order to establish a highly secure IoT Network for the whole project's lifetime the following conditions should be met:

- Transport Layer Security (TLS) protocol will be used for the communication between IoT Gateway and IML Cloud.
- All the communication among the IoT Network, which consists also the WSN, will be held in a local network level, satisfying the security requirements.
- TLS and/or OAuth2 will be used for any communication and data exchanged needed among the IML Cloud and the rest of the components of PARITY project, and specifically the BaaB App module that is included in the Prosumer Applications.

The specific steps that should be implemented to ensure the proper functionality of the aforementioned security framework has been described in detail in section 5 of the current version of the deliverable.

## 7.2 PARITY Blockchain and LEM/LFM Platform

### *7.2.1 Blockchain Platform and Smart Contracts*

In the blockchain platform, three main aspects have to be carefully taken into account under the security point of view: the consensus, the networking and data storage. The consensus, i.e. the capability to find an agreement among the nodes about how the next block will be constituted, is provided by the usage of a BFT (byzantine-fault-tolerant) algorithm. It guarantees a secure creation of block if the number of malicious nodes is lower than 33%. Regarding the P2P connections between the nodes, the communication is secured by an implementation of the Station-to-Station (STS) protocol [15]. Finally, the energy data stored on the blockchain are pseudonymized and, as a consequence, no malicious actors can obtain private information about the Prosumers and the compliance with the GDPR requirements is guaranteed.

### *7.2.2 Repository and off-chain tools*

The direct connection to DB using username and password can only be possible from the common LEM/LFM Repository component and on local computer. In addition, HTTP REST APIs will use encryption (TLS / HTTPS). LEM/LFM Repository must store users' passwords as hashes in DB (SHA-

256), and user role/type (affects access rights on application level). Moreover, it must, implement user's registration, deletion and user's login validation and password change web services. To accomplish access control and authentication through access tokens, an access token will be generated for each PARITY component. After successful validation of the access token, communication will be possible and the requested data will be included in the response.

## 7.3 PARITY Oracle

The Oracle component will be developed in order to facilitate the communication between the blockchain and the physical ecosystem. As one of the main components of PARITY, Oracle will communicate with Blockchain Agent, LEM/LFM Common Repository and LFM Off-chain tools in order to monitor and report securely and authorized the relative Key Performance Indicators to Smart Contracts, which are operated by Blockchain Agents.

Oracle will follow all the aforementioned security and authorization protocols that will be declared by the respective components (Blockchain & LFM). In particular, Oracle is able to encapsulate TLS/HTTPS protocol for secure transactions as well as OAuth2 for authorized transfer of data through REST APIs or Message Broking mechanisms (AMQP, MQTT, etc.).

## 7.4 PARITY Services and User Applications

### *7.4.1 EV Profiling and Smart Charging*

EV Profiling and Smart Charging component is responsible for integration and management of EV chargers and EVs. It exposes communication APIs for data exchange and stores data to the common Repository.

- Open Charge Point Protocol (OCPP) is used for data exchange between the component and the EV chargers
- REST API is used for communication with the EV platform. Basic authentication is used.
- Open Charging Point Interface (OCPI) is used for communication between different platforms. OCPI uses token-based authentication.
- IEC 60870-5-104 protocol can be used to communicate with DSO if needed.

### *7.4.2 Aggregator Toolset*

Aggregator Toolset includes UIs as well as back-end services components that are responsible for flexibility management and dispatching control commands to DERs and devices. It will not host a database itself, however, exchange of data with the Repository will be frequent. Access to UI will be allowed only to users registered as Aggregator after entering the correct username and password. The UI will display to the user only aggregated flexibility information, grouped either by Prosumers or by devices, in order to preserve privacy. Flexibility optimization services components will be able to communicate with the LEM/LFM Repository using the assigned access tokens. Aggregator Toolset will provide an interface to allow communication with external actors that are not part of the local energy community and market (TSO, BRP). Communication will be encrypted and will employ only requests for flexibility and the corresponding responses. Moreover, those actors will not have access to the LEM/LFM Repository or other database.

### *7.4.3 DSO Toolset*

The PARITY DSO Toolset is meant to be used by the distribution system operator. According to the architecture definition, it includes both a front-end allowing user interaction as well as back-end components for monitoring, management and control operations. As the DSO Toolset is also responsible for grid monitoring and management of the STATCOM device, it will utilize a dedicated database for

storing data out of LFM scope. In addition, connection with LEM/LFM Repository will be performed utilizing all security and privacy measures.

DSO Toolset implements role-based access control by supporting two types of users with different permissions: a regular "read-only" user for retrieving information and a user with full "read-write" rights for managing the STATCOM.

Regarding the use of secure protocols, TLS is utilized by either the REST API or MQTT protocol. Furthermore, successful validation of a client certificate is used for authenticating the client to the server. On the application level, the MQTT protocol supports the option to use username and password for authentication. Authorization is implemented by the MQTT server through the use of Access Control List (ACL) for mapping usernames to a set of topics and permissions. Lastly, enhanced security is achieved by the use of the encryption of the data through VPN.

### *7.4.4 Prosumer Applications*

Prosumer applications are UI applications that allow Prosumers to interact with the system. They are composed of three distinct UI modules: BaaB module, EV module, and Smart Marketplace module. Apart from providing the relevant data to the user and allowing performing control actions, additional functionalities such as notifications about the information that is collected and support for on-demand requests for data deletion will be implemented to ensure compliance with GDPR.

#### *7.4.4.1 BaaB App module*

BaaB module that will be developed under the framework of Prosumer applications and be deployed on HYPERTECH Cloud Server (Commissioning & Configuration, Environmental/Metering monitoring) is connected to two distinct types of user; commissioner and end-user. Commissioner can access the commissioning application only providing username and password while he is physically in the local network. On the other hand, end-users can access the monitoring app while they are on the local network without credentials. In case of remote access, the end-users are prompt to be validated and authenticated through the authorization framework using basic authentication (username, password). In that case, all the communications (REST APIs, message brokers) are accomplished through TLS protocol, using services that are hosted in the common LEM/LFM Repository. Utilizing a similar authorization framework for the visual analytics application, the end users are prompt to be validated and authenticated using basic authentication through a username and a password. Finally, regarding the communication and data exchange that is needed between the BaaB App module and the IoT Gateway, the authorization framework that will be implemented, is based on a TLS and/or Oauth2 framework, as described in section 7.1.

#### *7.4.4.2 EV module*

EV module is the web-based UI that will allow the user to interact with the EV Profiling and Smart Charging component. After successful authentication provided by the LEM/LFM Repository using username and password, EV module presents information of all EV chargers and/or EVs owned by the user. Authorization is performed based on the user type: (a) EV owner, (b) Charging point operator, (c) Administrator.

#### *7.4.4.3 Smart Marketplace module*

Smart Marketplace module is the web-based UI that will allow the user to view information related to his/her participation to the LEM/LFM. Indicative data that will be visualised are past transactions, wallet status, rewards earned, penalties etc. Secure communication with the off-chain tool's REST services using TLS will be implemented in order to retrieve the data after the user has been authenticated successfully via basic authentication by the LEM/LFM Repository services.

## 7.5 Interactions among Components

Detailed information about communication interfaces among PARITY components are described in the deliverable D3.5 PARITY System Architecture. Table 6 indicates whether privacy and security implementation is foreseen between communicating components.

**Table 6. Privacy and security implementation foreseen between communicating components.**

| Component A | Component B | Privacy | Security |
|---|---|---|---|
| IoT Gateway | Information Management Layer Cloud | ✓ | ✓ |
| PARITY Oracle | Blockchain Agent | | ✓ |
| PARITY Oracle | Off-chain tools | ✓ | ✓ |
| PARITY Oracle | LEM/LFM Repository | | ✓ |
| Blockchain Agent | Off-chain tools | ✓ | ✓ |
| Stationary Battery Manager | LEM/LFM Repository | | ✓ |
| PV Manager | LEM/LFM Repository | | ✓ |
| EV Profiling and Smart Charging | LEM/LFM Repository | | ✓ |
| EV Profiling and Smart Charging | Prosumer Applications | | ✓ |
| Prosumer Applications | LEM/LFM Repository | ✓ | ✓ |
| Aggregator Toolset | LEM/LFM Repository | | ✓ |
| Aggregator UI | Flexibility Optimization Services | ✓ | ✓ |
| DSO Toolset | LEM/LFM Repository | | ✓ |
| DSO Toolset | Aggregator Toolset | | ✓ |
| DSO Toolset | Interface TSO | | ✓ |

# 8. CONCLUSIONS

This report presents the specifications and all the required information related to the design and implementation of PARITY end-to-end security and privacy framework that will support all the actors involved. A privacy by design approach has been followed by considering data access, transfer and storage issues. Data Protection Impact Assessment was conducted for each pilot site as a first step towards the identification of the most critical security and privacy risks. Furthermore, compliance of the PARITY system with the GDPR has been considered, especially for issues related to users' privacy. In order to have a thorough view, relevant privacy and security guidelines proposed by the Smart Grid Task Force and other organisations, have been presented in this report and contributed to the identification of the privacy and security framework functionalities.

Apart from the enhanced security offered natively by the PARITY Blockchain platform, additional measures have been specified to be implemented by the other critical components of the PARITY system. The security access control framework that has been developed includes measures involving role-based access control, user authentication and authorization, use of secure communication protocols, such as TLS, and data encryption. With regard to privacy protection, anonymization and pseudonymization are the key measures that are going to be applied at both the IoT and LFM platform level. Lastly, the implementation of the privacy and security measures in each of the main PARITY components, as defined in the architecture design, have been presented.

# 9. REFERENCES

[1]. https://searchdatabackup.techtarget.com/definition/data-protection

[2]. V. Torra, (2017) Introduction. In: Data Privacy: Foundations, New Developments and the Big Data Challenge. Studies in Big Data, vol 28. Springer, Cham. https://doi.org/10.1007/978-3-319-57358-8_1

[3]. Collective, S. E. (2014). An introduction to the universal smart energy framework. Arnhem, The Netherlands, 1.

[4]. A. Cavoukian, Privacy by design. The 7 foundational principles in Privacy by Design. Strong privacy protection—now, and well into the future (2011). https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf, https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

[5]. https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp

[6]. https://securityintelligence.com/posts/the-gdpr-anniversary-compliance-matters-to-consumers/?_ga=2.86461853.446497060.1594723126-164030340.1594069315&_gac=1.15280068.1594735048.CjwKCAjwr7X4BRA4EiwAUXjbt6iWC0ii

[7]. USEF, "USEF: The privacy and security guideline", November 2015, https://www.usef.energy/app/uploads/2016/12/USEF_PrivacySecurityGuideline_3nov15.pdf

[8]. Sample DPIA template, 2018, Accessible at https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

[9]. Smart Grid Task Force, Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, September 2018, Accessible at https://ec.europa.eu/energy/content/data-protection-impact-assessment-template-smart-grid-and-smart-metering-systems_en

[10]. https://gdpr-info.eu/art-4-gdpr/

[11]. https://www.termsfeed.com/blog/gdpr-pseudonymization-anonymization/#Advantages_Of_Data_Masking

[12]. Smart Grids Task Force – EG2, "Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management", Final report, June 2019, URL: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

[13]. ENISA Smart Grid Task Force - EG2, "Proposal for a list of security measures for smart grids", 2014, https://ec.europa.eu/energy/sites/ener/files/documents/20140409_enisa.pdf

[14]. ETSI EN 303 645 European Standard on Cyber Security for Consumer Internet of Things: Baseline requirements, 2020, v2.1.0, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

[15]. Diffie, W., Van Oorschot, P. C., & Wiener, M. J. (1992). Authentication and authenticated key exchanges. Designs, Codes and cryptography, 2(2), 107-125.

# ANNEX A: Data Protection Impact Assessment Template

# Data Protection Impact Assessment Template

## Section 1. DPIA Introduction

**This document is intended to be used by Data Controllers for conducting a thorough Data Protection Impact Assessment (DPIA), which describes the envisaged Data Processing, an assessment of the Risks to the rights and freedoms of data subjects, the measures, safeguards, and controls and mechanisms envisaged to address the Risks, ensuring the protection of Personal Data.**

**The GDPR foresees the DPIA as a key instrument to enhance Data Controllers' accountability as it helps controller not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the GDPR. If a decision of the Data Controller or Processor leads to an implementation of new technologies, a DPIA has to be conducted. Within PARITY project, new technologies involved are Internet of Things, Blockchain and the smart meter environment both at DSO and prosumer level.**

**PARITY addresses the "structural inertia" of Distribution Grids and aims to enable the set-up and operation of Local Flexibility Markets at the distribution network level. The project will target at developing Local Flexibility Markets & Smart Energy Grids through peer-to-peer and decentralized intelligence in a human-centric manner. The main objectives are to provide: (a) A DER flexibility ecosystem seamlessly integrating Heterogeneous DER within a Unified Flexibility Management Framework; (b) A Storage-as-a-Service framework which will combine Actual Storage (EVs and batteries) and Virtual Energy Storage (Power-to-Heat); (c) A Smart Contracts Enabled Local Flexibility Market Platform through integration of IoT and Blockchain technologies; (d) Smart Grid monitoring and management tools to enable the DSO to optimally manage the low voltage distribution network.**

**Within PARITY, different types of data will be collected, such as data from surveys and interviews involving participants, raw data from pilot sites' sensors and devices, data entered to the system by the participants (e.g. preferences), and data generated from software components that will be developed within the project.**

## Section 2. Description of processing

**For ensuring proper data collection, data transfers to database will be automated and secure. Regarding user data that will be stored, such as energy consumption and generation, usage patterns, thermal comfort profiles, etc., they will be anonymized. User identification data may be stored and used only for problem solving during the development phase. The system will allow deletion of selected data upon request.**

**Safe data sharing is foreseen by fully enforcing and protecting user rights. For the data that will be shared only among the consortium members, authorization and authentication mechanisms will be used in order to restrict access and ensure that only the appropriate users can retrieve the data. Specific not sensitive and anonymized data may be made publicly available for scientific purpose. Special category data, e.g. personal data revealing ethnic origin, political opinions, genetic data, data concerning health, or criminal offence data, as defined in GDPR, are not relevant to the project and will not be collected.**

**The main purpose of the processing is to evaluate the different solutions that will be developed within PARITY: solutions for prosumers, aggregators, DSOs, and other actors. Indicative examples of performance indicators are the amount of energy consumption reduction, increase in RES utilization, and peak load reduction. Moreover, part of the collected data will be processed manually or in automated way, in order to be used as input to algorithms (e.g. machine learning, optimization algorithms).**

**Estimated number of individuals affected by data processing:_____**

**Geographical area that data collection and processing covers:_____**

**Nature of relationship with the individuals:**
**_____**

**Additional information:**
**_____**
**_____**
**_____**

## Section 3. Consultation process

**The Ethical Advisory Board has been formed within PARITY to provide ongoing support concerning ethical and legal issues to the consortium, including support on privacy issues related to data collection at the pilot sites.**

**Information security experts or any other experts planned to consult: _____**

**_____**

| Section 4. Necessity and proportionality |
|---|
| **PARITY will collect and store personal data only if it is absolutely necessary for achieving the project aim. To ensure data quality, pre-processing and data cleaning methods will be applied to the data that are automatically collected from the devices and sensors. Regarding data minimization, only personal data actually needed for our purposes will be collected. Stored data will be reviewed periodically, in order to delete data that are no longer needed.**<br><br>**Informed consent procedures will be implemented for the participation of humans. The pilot and the level of privacy infringement will be described to the people involved. Furthermore, consent forms will be prepared by the consortium and filled by the participants of the pilot sites. The participants will be informed in detail about the data that will be collected and the data that will be processed. In case a candidate participant wants to exercise his/her right not to know, he/she will be excluded from the pilot.**<br><br>**Additional information:**<br>_____<br>_____<br>_____ |

| Section 5. Risk identification and assessment | | | |
|---|---|---|---|
| **Risk** | **Likelihood of harm**<br>**(1 – 5. Negligible to Maximum)** | **Severity of harm**<br>**(1 – 5. Negligible to Maximum)** | **Overall risk priority**<br>**(1 – 4)**<br>***consult ANNEX A** |
| **Illegitimate processing of Personal Data** | | | |
| **No lawfulness of processing**<br>***To process Personal Data it is necessary to have a legal basis defined in Art.6 GDPR or the national Data Protection laws (e.g. consent of the data subject, contract with the data subject, documented legitimate interest of the Data Controller, legal requirements)*** | | | |
| **Collection exceeding purpose**<br>***More Personal Data is collected than what is*** | | | |

| | | | |
|---|---|---|---|
| ***necessary to achieve a specified purpose.*** | | | |
| **Unclear responsibilities for Data Processing**<br>***It is not clear to data subjects what parties are involved in the processing of data and their respective roles.*** | | | |
| **The protection of data is compromised outside the European Economic Area (EEA)**<br>***There is a risk that smart metering data may be at risk if sent outside of the EEA. Another risk is that Personal Data like metering data gives inside information about vital infrastructures in an unknown, maybe untruthful environment.*** | | | |
| **Inadequate information of the data subject** | | | |
| **Incomplete information**<br>***The information provided to the data subject on the purpose and use of data is not complete.*** | | | |
| **Violation of the data subject's rights** | | | |
| **Inability to execute individual rights (inspection rights)**<br>***If data are going to be held by multiple Data Controllers, then consumers should have a means by which to access these data from multiple sources using a single subject access request.*** | | | |
| **Prevention of objections** | | | |

| | | | |
|---|---|---|---|
| ***Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible.*** | | | |
| **A lack of transparency for automated individual decisions**<br><br>***Automated processing of Personal Data intended to evaluate certain personal aspects or conduct is used but the data subjects are not informed about the logic of the decision-making.*** | | | |
| **Lack of correction of Personal Data**<br><br>***There is no way for the data subject to initiate a correction of his data according to article 16 of the GDPR. The Data Controller and / or Data Processor are not sufficiently prepared to respond to such requests.*** | | | |
| **Lack of erasure of Personal Data.**<br><br>***There is no way for the data subject to initiate an erasure of his data according to article 17 of the GDPR. The Data Controller and / or Data Processor are not sufficiently prepared to respond to such requests.*** | | | |
| **Compliance violations in the contracts** | | | |
| **Missing or incorrect contractual Data Protection clause.**<br><br>***It is required to have a Data Protection clause in contracts for Data Processing on*** | | | |

| | | | |
|---|---|---|---|
| ***behalf. The content of the Data Protection clause is legally required and different in the EU countries. There are additional requirements for Data Processors in third Countries.*** | | | |
| **Personal Data integrity loss** | | | |
| **Lack of quality of data for the purpose of use.**<br>***If data is used for certain processes it should be adequate.*** | | | |
| **Inability to respond to requests for subject access, correction or deletion of data in a timely and satisfying manner.**<br>***The data is distributed across several business units and an integrated overview cannot be made within a short time frame.*** | | | |
| **Damage to individual** | | | |
| **Discrimination** | | | |
| **Identify Theft or Fraud** | | | |
| **Financial loss** | | | |
| **Other significant economic or social disadvantage** | | | |
| **Physical attack (deliberate/ intentional)** | | | |
| **Fraud**<br>***Fraud committed by humans. I.e. Forgery of paper documents.*** | | | |
| **Sabotage** | | | |

| | | | |
|---|---|---|---|
| ***Intentional actions (non-fulfilment or defective fulfilment of personal duties) aimed to cause disruption or damage to IT assets.*** | | | |
| **Vandalism**<br>***Act of physically damaging IT assets.*** | | | |
| **Theft (of devices, storage media and documents)**<br>***Stealing information or IT assets. Robbery. I.e. theft of a laptop from a hotel room; loss of an electronic storage device.*** | | | |
| **Information leak /sharing**<br>***Sharing information with unauthorized entities. Loss of information confidentiality due to intentional human actions (e.g., information leak may occur due to loss of paper copies of confidential information).*** | | | |
| **Unauthorized physical access / Unauthorized entry to premises** | | | |
| **Coercion, extortion or corruption**<br>***Actions following acts of coercion, extortion or corruption.*** | | | |
| **Damage from the warfare**<br>***Threats of direct impact of warfare activities.*** | | | |
| **Terrorist attack** | | | |
| **Unintentional damage / loss of information or IT assets** | | | |

| | | | |
|---|---|---|---|
| **Information leak /sharing due to human error**<br><br>***Information leak / sharing caused by humans, due to their mistakes or working conditions. I.e. high workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities etc.*** | | | |
| **Erroneous use or administration of devices and systems**<br><br>***Information leak / sharing / damage caused by misuse of IT assets (lack of awareness of application features) or wrong / improper IT assets configuration or management.*** | | | |
| **Unintentional change of data in an information system**<br><br>***Loss of information integrity due to human error (information system user mistake).*** | | | |
| **Inadequate design and planning or improper adaptation**<br><br>***Threats caused by improper IT assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors). I.e. the implemented logging mechanism is insufficient. It does not log administrative processes.*** | | | |

| | | | |
|---|---|---|---|
| **Loss of (integrity of) sensitive information**<br>***Threats of losing information or data, or changing information classified as sensitive.*** | | | |
| **Disaster (natural, environmental)** | | | |
| **Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy winds, fire, water etc.)**<br>***Threats of damage to information assets caused by natural or environmental factors.*** | | | |
| **Failures/ Malfunction** | | | |
| **Failure of devices or systems**<br>***Threat of failure/malfunction of IT supporting infrastructure (i.e. degradation of quality, improper working parameters, jamming). The cause of a failure is mostly an internal issue.*** | | | |
| **Failure or disruption of communication links (communication networks)**<br>***Threat of failure or malfunction of communications links.*** | | | |
| **Failure or disruption of main supply**<br>***Threat of failure or disruption of supply required for information systems. I.e. Loss of power can harm hardware and software and lead to unavailability of*** | | | |

| | | | |
|---|---|---|---|
| ***computing systems, network equipment and disruption of Smart Grid devices.*** | | | |
| **Malfunction of equipment (devices or systems)**<br>***Threat of malfunction of IT hardware and/or software assets or its parts. I.e. Errors during updates, configuration or maintenance; replacement of components, etc.*** | | | |
| **Outages** | | | |
| **Absence of personnel**<br>***Unavailability of key personnel and their competences.*** | | | |
| **Loss of support services**<br>***Unavailability of support services required for proper operation of the information system.*** | | | |
| **Internet or Network outage**<br>***Unavailability of the Internet or network connection.*** | | | |
| **Eavesdropping/ Interception/ Hijacking** | | | |
| **Interception of information**<br>***Threat of interception of information that is improperly secured in transmission or by improper actions of staff. I.e. watching a person's screen without them knowing while on the train; taking a photo of a screen; geo-location of hardware; remote detection of electromagnetic signals, shoulder-surfing etc.*** | | | |

| | | | |
|---|---|---|---|
| **Interfering radiation**<br>***Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source.*** | | | |
| **Replay of messages**<br>***Threat in which valid data transmission is maliciously or fraudulently repeated or delayed.*** | | | |
| **Man in the middle / Session hijacking**<br>***Threats that relay or alter communication between two parties. I.e. interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.*** | | | |
| **Nefarious Activity / Abuse** | | | |
| **Identity theft (Identity Fraud/ Account)**<br>***Threat of identity theft action.*** | | | |
| **Denial of service**<br>***Threat of service unavailability due to massive requests for services.*** | | | |
| **Malicious code/ software/ activity**<br>***Threat of malicious code or software execution. I.e. Software Key-logger logs all keystrokes and/or Trojan sends commands and data to attacker's computer system.*** | | | |
| **Manipulation of hardware and software** | | | |

| | | | |
|---|---|---|---|
| ***Threat of unauthorised manipulation of hardware and software. I.e: Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, etc.*** | | | |
| **Misuse of information/ information systems**<br><br>***Threat of nefarious action due to misuse of information systems. I.e. addition of incompatible hardware resulting in malfunctions; changing of components essential to the owner operation of an application, etc.*** | | | |
| **Unauthorized activities**<br><br>***Threat of nefarious action due to unauthorised activities. I.e. Installation of Key-loggers; key-logger logs all keystrokes. Allows attackers to reuse usernames, passwords, compromising data to be observed and searched for specific words, sentences etc.*** | | | |
| **Compromising confidential information**<br><br>***Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.*** | | | |
| **Abuse of authorizations**<br><br>***Threat of using authorised access to perform illegitimate actions. I.e. content scanning; illegitimate cross-referencing*** | | | |

| | | | | |
|---|---|---|---|---|
| ***of data; raising of privileges, wiping of usage tracks; sending of spam via an e-mail program; misuse of network functions; Access rights are not revoked when they are no longer necessary.*** | | | | |
| **Other** | | | | |
| ***<Add other risks here>*** | | | | |
| **Section 6. Measures identification** | | | | |
| **Identify the measures you could take to reduce or eliminate risks identified with overall risk priority 1 to 3 in previous section. Note that the actions/measures must be compliant with the GDPR requirements. A list of indicative measures is provided in ANNEX B.** | | | | |
| **Risk** | **Measures to reduce or eliminate risk**<br>**(including assuring compliance with GDPR requirements)** | **Effect on risk**<br>**(Eliminated, Reduced, Accepted)** | **Residual risk**<br>**{Likelihood, Severity}**<br>**Risk Priority**<br>**(1 - 4)** | **Measure approved**<br>**(Yes/No)** |
| **Illegitimate processing of Personal Data** | | | | |
| **No lawfulness of processing**<br>***To process Personal Data it is necessary to have a legal basis defined in Art.6 GDPR or the national Data Protection laws (e.g. consent of the data subject, contract with the data subject, documented legitimate interest of the Data Controller, legal requirements)*** | | | | |
| **Collection exceeding purpose** | | | | |

| | | | | |
|---|---|---|---|---|
| ***More Personal Data is collected than what is necessary to achieve a specified purpose.*** | | | | |
| **Unclear responsibilities for Data Processing**<br>***It is not clear to data subjects what parties are involved in the processing of data and their respective roles.*** | | | | |
| **The protection of data is compromised outside the European Economic Area (EEA)**<br>***There is a risk that smart metering data may be at risk if sent outside of the EEA. Another risk is that Personal Data like metering data gives inside information about vital infrastructures in an unknown, maybe untruthful environment.*** | | | | |
| **Inadequate information of the data subject** | | | | |
| **Incomplete information**<br>***The information provided to the data subject on the purpose and use of data is not complete.*** | | | | |
| **Violation of the data subject's rights** | | | | |
| **Inability to execute individual rights (inspection rights)**<br>***If data are going to be held by multiple Data Controllers, then consumers should have a means by which to access these data from multiple sources using a single subject access request.*** | | | | |

| | | | | |
|---|---|---|---|---|
| **Prevention of objections**<br>***Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible.*** | | | | |
| **A lack of transparency for automated individual decisions**<br>***Automated processing of Personal Data intended to evaluate certain personal aspects or conduct is used but the data subjects are not informed about the logic of the decision-making.*** | | | | |
| **Lack of correction of Personal Data**<br>***There is no way for the data subject to initiate a correction of his data according to article 16 of the GDPR. The Data Controller and / or Data Processor are not sufficiently prepared to respond to such requests.*** | | | | |
| **Lack of erasure of Personal Data**<br>***There is no way for the data subject to initiate an erasure of his data according to article 17 of the GDPR. The Data Controller and / or Data Processor are not sufficiently prepared to respond to such requests.*** | | | | |
| **Compliance violations in the contracts** | | | | |
| **Missing or incorrect contractual Data Protection clause** | | | | |

| | | | | |
|---|---|---|---|---|
| ***It is required to have a Data Protection clause in contracts for Data Processing on behalf. The content of the Data Protection clause is legally required and different in the EU countries. There are additional requirements for Data Processors in third Countries.*** | | | | |
| **Personal Data integrity loss** | | | | |
| **Lack of quality of data for the purpose of use**<br>***If data is used for certain processes it should be adequate.*** | | | | |
| **Inability to respond to requests for subject access, correction or deletion of data in a timely and satisfying manner**<br>***The data is distributed across several business units and an integrated overview cannot be made within a short time frame.*** | | | | |
| **Damage to individual** | | | | |
| **Discrimination** | | | | |
| **Identify Theft or Fraud** | | | | |
| **Financial loss** | | | | |
| **Other significant economic or social disadvantage** | | | | |
| **Physical attack (deliberate/ intentional)** | | | | |
| **Fraud**<br>***Fraud committed by humans. I.e. Forgery of paper documents.*** | | | | |

| | | | | |
|---|---|---|---|---|
| **Sabotage**<br>***Intentional actions (non-fulfilment or defective fulfilment of personal duties) aimed to cause disruption or damage to IT assets.*** | | | | |
| **Vandalism**<br>***Act of physically damaging IT assets.*** | | | | |
| **Theft (of devices, storage media and documents)**<br>***Stealing information or IT assets. Robbery. I.e. theft of a laptop from a hotel room; loss of an electronic storage device.*** | | | | |
| **Information leak /sharing**<br>***Sharing information with unauthorized entities. Loss of information confidentiality due to intentional human actions (e.g., information leak may occur due to loss of paper copies of confidential information).*** | | | | |
| **Unauthorized physical access / Unauthorized entry to premises** | | | | |
| **Coercion, extortion or corruption**<br>***Actions following acts of coercion, extortion or corruption.*** | | | | |
| **Damage from the warfare**<br>***Threats of direct impact of warfare activities.*** | | | | |
| **Terrorist attack** | | | | |

| **Unintentional damage / loss of information or IT assets** | | | | |
|---|---|---|---|---|
| **Information leak /sharing due to human error**<br>***Information leak / sharing caused by humans, due to their mistakes or working conditions. I.e. high workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities etc.*** | | | | |
| **Erroneous use or administration of devices and systems**<br>***Information leak / sharing / damage caused by misuse of IT assets (lack of awareness of application features) or wrong / improper IT assets configuration or management.*** | | | | |
| **Unintentional change of data in an information system**<br>***Loss of information integrity due to human error (information system user mistake).*** | | | | |
| **Inadequate design and planning or improper adaptation**<br>***Threats caused by improper IT assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors). I.e. the implemented logging mechanism is insufficient. It does not log administrative processes.*** | | | | |

| | | | | |
|---|---|---|---|---|
| **Loss of (integrity of) sensitive information**<br>***Threats of losing information or data, or changing information classified as sensitive.*** | | | | |
| **Disaster (natural, environmental)** | | | | |
| **Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy winds, fire, water etc.)**<br>***Threats of damage to information assets caused by natural or environmental factors.*** | | | | |
| **Failures/ Malfunction** | | | | |
| **Failure of devices or systems**<br>***Threat of failure/malfunction of IT supporting infrastructure (i.e. degradation of quality, improper working parameters, jamming). The cause of a failure is mostly an internal issue.*** | | | | |
| **Failure or disruption of communication links (communication networks)**<br>***Threat of failure or malfunction of communications links.*** | | | | |
| **Failure or disruption of main supply**<br>***Threat of failure or disruption of supply required for information systems. I.e. Loss of power can harm hardware and software and lead to unavailability of*** | | | | |

| | | | | |
|---|---|---|---|---|
| ***computing systems, network equipment and disruption of Smart Grid devices.*** | | | | |
| **Malfunction of equipment (devices or systems)**<br>***Threat of malfunction of IT hardware and/or software assets or its parts. I.e. Errors during updates, configuration or maintenance; replacement of components, etc.*** | | | | |
| **Outages** | | | | |
| **Absence of personnel**<br>***Unavailability of key personnel and their competences.*** | | | | |
| **Loss of support services**<br>***Unavailability of support services required for proper operation of the information system.*** | | | | |
| **Internet or Network outage**<br>***Unavailability of the Internet or network connection.*** | | | | |
| **Eavesdropping/ Interception/ Hijacking** | | | | |
| **Interception of information**<br>***Threat of interception of information that is improperly secured in transmission or by improper actions of staff. I.e. watching a person's screen without them knowing while on the train; taking a photo of a screen; geo-location of hardware; remote detection of electromagnetic signals, shoulder-surfing etc.*** | | | | |

| | | | | |
|---|---|---|---|---|
| **Interfering radiation**<br>***Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source.*** | | | | |
| **Replay of messages**<br>***Threat in which valid data transmission is maliciously or fraudulently repeated or delayed.*** | | | | |
| **Man in the middle / Session hijacking**<br>***Threats that relay or alter communication between two parties. I.e. interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.*** | | | | |
| **Nefarious Activity/ Abuse** | | | | |
| **Identity theft (Identity Fraud/ Account)**<br>***Threat of identity theft action.*** | | | | |
| **Denial of service**<br>***Threat of service unavailability due to massive requests for services.*** | | | | |
| **Malicious code/ software/ activity**<br>***Threat of malicious code or software execution. I.e. Software Key-logger logs all keystrokes and/or Trojan sends commands and data to attacker's computer system.*** | | | | |
| **Manipulation of hardware and software** | | | | |

| | | | | |
|---|---|---|---|---|
| ***Threat of unauthorised manipulation of hardware and software. I.e: Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, etc.*** | | | | |
| **Misuse of information/ information systems**<br><br>***Threat of nefarious action due to misuse of information systems. I.e. addition of incompatible hardware resulting in malfunctions; changing of components essential to the owner operation of an application, etc.*** | | | | |
| **Unauthorized activities**<br><br>***Threat of nefarious action due to unauthorised activities. I.e. Installation of Key-loggers; key-logger logs all keystrokes. Allows attackers to reuse usernames, passwords, compromising data to be observed and searched for specific words, sentences etc.*** | | | | |
| **Compromising confidential information**<br><br>***Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.*** | | | | |
| **Abuse of authorizations**<br><br>***Threat of using authorised access to perform illegitimate actions. I.e. content scanning; illegitimate cross-referencing*** | | | | |

| | | | | |
|---|---|---|---|---|
| ***of data; raising of privileges, wiping of usage tracks; sending of spam via an e-mail program; misuse of network functions; Access rights are not revoked when they are no longer necessary.*** | | | | |
| **Other** | | | | |
| | | | | |

| **Section 7. Check of GDPR requirements** | | |
|---|---|---|
| **Provisions** | **Yes/No** | **Rationale** |
| **The Principles relating to processing of Personal Data have been fulfilled [art.5]** | | |
| **Purpose limitation** | | |
| **Data minimization** | | |
| **Storage limitation** | | |
| **Integrity and confidentiality** | | |
| **Data is accurate and kept up-to-date** | | |
| **The processing is based on Lawfulness conditions provided by GDPR [art. 6]** | | |
| **Where the processing is based on consent, it is possible to demonstrate that the data subject has consented to processing of his or her Personal Data [art. 7]** | | |

| | | |
|---|---|---|
| **Processing of special categories of Personal Data is performed adopting all the measures provided by GDPR [art. 9]** | | |
| **The controller provided information to the data subject [art.13,14]** | | |
| **The right of access by the data subject is guaranteed [art. 15]** | | |
| **The right to rectification is guaranteed [art. 16]** | | |
| **The right to erasure is guaranteed [art. 17]** | | |
| **The right to restriction of processing is guaranteed [art .18]** | | |
| **Has ever been sent to the recipients of the Personal Data a notification when the data subject requested a rectification, erasure or restriction of processing? Is a procedure available? [art. 19]** | | |
| **The right of data portability is guaranteed [art. 20]** | | |
| **The right to object to a processing is guaranteed [art. 21]** | | |
| **The right to object to a decision based solely on automated processing including profiling (if applicable) [art. 22]** | | |
| **Principles of data protection by design and data protection by default are applied [art. 25]** | | |
| **An agreement with eventual joint controllers is established [art.26]** | | |
| **The processor has been appointed and provides guarantees to implement appropriate technical and organisational measures and ensure the protection of the rights of the data subjects [art. 28]** | | |
| **Anybody in charge of the processing is acting under instructions of the controller [art. 29]** | | |

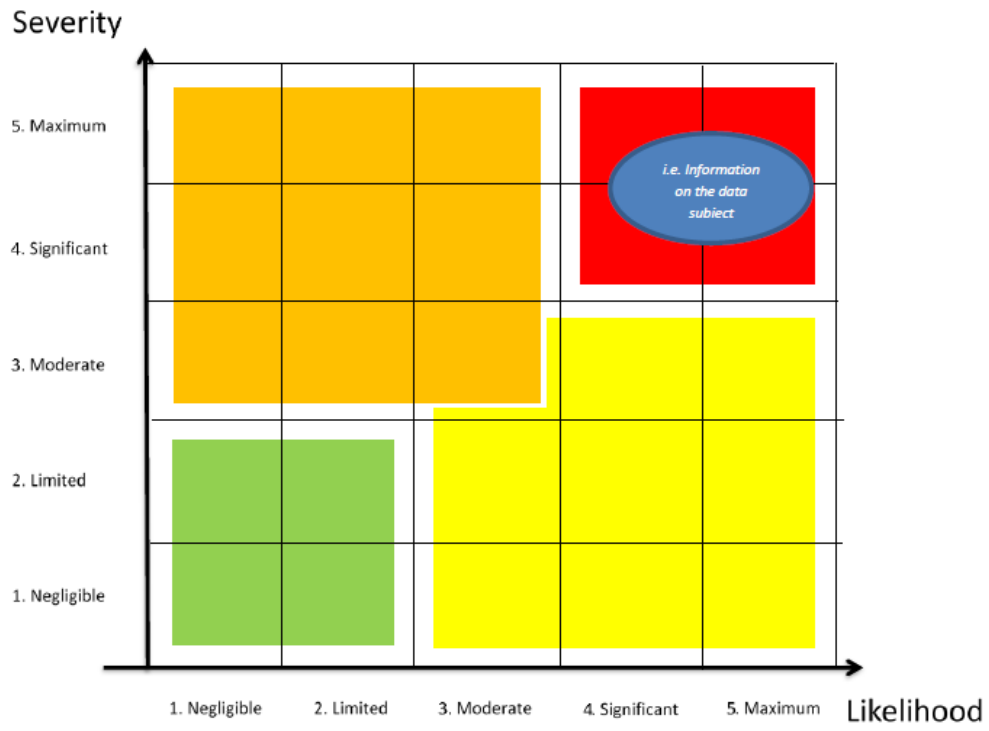
| | | |
|---|---|---|
| **Records of processing activities are provided [art. 30]** | | |
| **Security measures have been adopted [art. 32]** | | |
| **Procedures have been adopted for dealing with data breaches and notification of breaches to DPA or to the affected individuals (if applicable) [art. 33 and 34]** | | |
| **A pre-existing Data Protection Impact Assessment had already been done [art. 35]** | | |
| **A Prior Consultation already took place [art. 36]** | | |
| **A DPO has been appointed [art. 37]** | | |
| **Data Controller or Data Processor abides to a Code of Conduct [art. 40]** | | |
| **Data Controller or Data processor has received certification [art. 42]** | | |
| **Transfer of Personal Data outside the EU is performed accordingly to the GDPR provisions [art. 44-49]** | | |

| **Section 8. Sign off and record outcomes** | | |
|---|---|---|
| **Item** | **Name/Date** | **Notes** |
| **Measures approved by:** | | **Integrate actions back into project plan, with date and responsibility for completion** |
| **Residual risks approved by:** | | **If accepting any residual high risk, consult the ICO before going ahead** |
| **DPO advice provided:** | | **DPO should advise on compliance, step 6 measures and whether processing can proceed** |
| **Summary of DPO advice:** | | |

| | | |
|---|---|---|
| **DPO advice accepted or overruled by:** | | **If overruled, you must explain your reasons** |
| **Comments:** | | |
| **Consultation responses reviewed by:** | | **If your decision departs from individuals' views, you must explain your reasons** |
| **Comments:** | | |
| **This DPIA will kept under review by:** | | **The DPO should also review ongoing compliance with DPIA** |

## ANNEX A – RISK PRIORITY

Overall risk priority (1: "red" to 4: "green") to be calculated according to the diagram below:




## ANNEX B – List of Possible Controls

| No | Name of a Control | Control's Objective |
|---|---|---|
| **1.** | **Managing contracts between Data Controllers and Data Processors** | to reduce the risks associated with missing or incorrect contractual Data Protection clauses |
| **2.** | **Managing third parties with legitimate access to Personal Data** | to reduce the risk that legitimate access to Personal Data by third parties may pose to the data subjects' rights and freedoms. |
| **3.** | **Monitoring logical access controls** | to limit the risks that unauthorized persons will access Personal Data electronically. |
| **4.** | **Partitioning Personal Data** | to reduce the possibility that Personal Data can be correlated and that a breach of all Personal Data may occur. |
| **5.** | **Encrypting Personal Data** | to make Personal Data unintelligible to anyone without access authorization. |
| **6.** | **Anonymizing Personal Data** | to remove identifying characteristics from Personal Data. |
| **7.** | **Protecting Personal Data archives** | to define all procedures for preserving and managing the electronic archives containing the Personal Data. |

| | | |
|---|---|---|
| **8.** | **Managing Personal Data violations** | to have an operational organisation that can detect and treat incidents that may affect the data subjects' civil liberties and privacy. |
| **9.** | **Tracing the activity on the IT system** | to allow early detection of incidents involving Personal Data and to have information that can be used to analyse them or provide proof in connection with investigations. |
| **10.** | **Combating malicious codes** | to protect access to public (Internet) and uncontrolled (partner) networks, workstations and servers from malicious codes that could affect the security of Personal Data. |
| **11.** | **Reducing software vulnerabilities** | to reduce the possibility to exploit software properties (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.) to adversely affect Personal Data. |
| **12.** | **Reducing hardware vulnerabilities** | to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect Personal Data. |
| **13.** | **Reducing the vulnerabilities of computer communications networks** | to reduce the possibility to exploit communications networks properties (wired networks, Wi-Fi, radio waves, fibre optics, etc.) to adversely affect Personal Data. |
| **14.** | **Reducing the vulnerabilities of paper documents** | to reduce the possibility to exploit paper documents properties to adversely affect Personal Data. |
| **15.** | **Reducing vulnerabilities related to the circulation of paper documents** | to reduce the possibility to exploit paper document circulation properties (within an organisation, delivery by vehicle, mail delivery, etc.) to adversely affect Personal Data. |
| **16.** | **Create procedures to address CoT and CoS** | to ensure that after such a change, no Personal Data is available |
| **17.** | **Permitting the exercise of the right to object** | to ensure that individuals have an opportunity to object to the use of their Personal Data. |
| **18.** | **Monitoring the integrity of Personal Data** | to be warned in the event of an unwanted modification or disappearance of Personal Data. |
| **19.** | **Reducing the vulnerabilities of individuals** | to reduce the possibility to exploit people (employees, individuals |

| | | |
|---|---|---|
| | | who are not part of an organisation but are under its responsibility, etc.) by adversely affecting Personal Data. |
| **20.** | **No collection of identifiable information, only pseudonyms, or anonym data** | to prevent identification of the data subject through collected data. |
| **21.** | **Active measure to preclude the use of particular data-items in the making of particular decisions** | to ensure that decisions are made based only on due data-items. |
| **22.** | **Limits on the use of information for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose** | to ensure that information is used for the specified purpose and for nothing more than that. |
| **23.** | **Active measures to preclude the disclosure of particular data-items** | to ensure that only required and permitted data-items are disclosed. |
| **24.** | **Minimization of Personal Data retention by destroying it as soon as the transaction for which it is needed is completed** | to ensure compliance with legislation and to prevent misuse of Personal Data. |
| **25.** | **Destruction schedules for personal information** | to ensure compliance with legislation and to prevent misuse of Personal Data. |
| **26.** | **Use of mathematical methods without collecting and registration source data to reach goals** | to avoid collection of non-authorized data without prejudice to reach goals. |
| **27.** | **Give the individual control over his or her data, for example by a secured website portal** | to ensure that the individual has control over his or her data according to his rights and responsibilities. |
| **28.** | **Introduction automated controls on the data quality** | to ensure that data quality is monitored and maintained on a regular basis. |
| **29.** | **Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers** | to ensure that clients have a way of communicating their requests and complaints and to ensure that these are timely and adequately addressed. |
| **30.** | **Audit** | a generic control to ensure that all implemented Controls are in place |