UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Computer Science Curriculum

Sander Truu

# Tool-Supported Privacy Analysis of Smart Parking

Bachelor's Thesis (9 ECTS)

Supervisor(s): Mariia Bakhtina
Raimundas Matulevičius

Tartu 2024

## Tool-Supported Privacy Analysis of Smart Parking

**Abstract:**

Organisations today deal with a lot of data processing which introduces new risks such as data theft, data manipulation or sensitive information exposure. Implementing additional security features requires extra resources from organisations like additional personnel, time and money. General Data Protection Regulation (GDPR) regulates data processing and sets the requirements for companies to follow in the European Union (EU). It has been around for 8 years yet there are no certain procedures or frameworks for organisations to follow that could be used for privacy analysis of business processes. To support organisations with the problem we demonstrate the tool-supported privacy analysis method, which uses the DPO Tool and Pleak tool on smart parking business processes to identify privacy violations during data processing. This thesis validates the proposed method for analysing business processes' privacy issues. It gives an overview of the tools on a real-life scenario, enabling the method to be used in the future. We provide privacy-enhanced business process models along with a detailed privacy analysis which demonstrates the readiness of the method. As a result, the thesis provides a tool-supported analysis of smart parking, demonstrating the use of the selected tools in adding privacy-preserving measures to business processes. Through this process we validate the usability of the method and propose privacy-preserving smart parking process redesign options. The method used can be employed by companies to conduct privacy analysis.

**Keywords:**
General Data Protection Regulation (GDPR), smart parking, personal data protection, privacy-enhancing technologies

**CERCS: T120** – Systems engineering, computer technology

## Targa parkimise privaatsuse analüüs tööriistade toel

**Lühikokkuvõte:**

Organisatsioonid täna tegelevad suures mahus andmete töötlusega, mille tõttu puutuvad nad kokku uute riskidega nagu andmevargus, andmete manipulatsioon või tundlikke andmete leke. Turvameetmete implementeerimine nõuab organisatsioonidelt ressursse nagu tööjõud, aeg ja raha. Isikuandmete kaitse üldmäärus reguleerib andmete töötlust ning seab paika nõuded ettevõtetele, mida peab Euroopa Liidus järgima. See on eksisteerinud ligi 8 aastat, kuid ettevõtetele pole konkreetseid protseduure ega raamistikke ette nähtud, mis oleksid rakendatavad äriprotsesside privaatsusanalüüsides. Et toetada organisatsioone selle probleemiga, demonstreerime tööriistadele toetuvat privaatsusanalüüsi meetodit, mille käigus kasutame DPO tööriista ning Pleak tööriista targa parkimise äriprotsesside analüüsimiseks, et leida privaatsuse rikkumisi andmete töötlemisel. See töö valideerib väljapakutud meetodit äriprotsesside analüüsimiseks. Töös saab ülevaate tööriistadest ja nende kasutusest reaalse domeeni peal, mis võimaldab seda raamistikku tulevikus kasutada ka teiste domeenide peal. Töö käigus jõuame privaatsuskaitse tehnoloogiatega täiendatud äriprotsessi mudeliteni ning detailse privaatsusanalüüsini, mis näitab meetodi võimalusi ning kasutatavust. Töö tulemuseks on targa parkimise süsteemi privaatsusanalüüs, mis annab ülevaate meetodi kasutamisest äriprotsesside analüüsimiseks ja täiendamiseks. Meetodi rakendamise abil valideerime meetodi kasutatavust ning pakume targa parkimise süsteemi jaoks välja privaatsuskaitse võimalused. Töös kasutatud meetod on üheks võimaluseks organisatsioonidele äriprotsesside privaatsusanalüüsi läbiviimiseks.

**Võtmesõnad:**

Isikuandmete kaitse üldmäärus (GDPR), tark parkimine, isikuandmete kaitse, privaatsuskaitse tehnoloogiad

**CERCS: T120** – Süsteemitehnoloogia, arvutitehnoloogia

## Acknowledgements

This work is part of the Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) project funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

# Contents

# 1 Introduction

As the world develops, the parking service is developing into an online service that is increasingly integrated into modern cities [1]. Users can access the parking service through an application on their smartphone or car panels. This allows users to park their vehicles in urban areas, reducing traffic and time spent finding a parking spot. Parking fees differ according to different zones, periods and daily times. The smart parking service uses prepayment and intelligent detection of free parking slots, allowing users to interact remotely and in advance with the parking system. This means these systems collect and process user data such as location, payment information and parking times. Processing the mentioned data assists the smart parking system in providing the aforementioned benefits. To trust these services and integrate them into the cities, the users need to be sure that their personal data is protected. While information privacy assurance is regulated, organisations are responsible for securing both user data and organisational information to meet the requirements. Data leakages and unauthorised access to the system might result in user tracking and linking, malicious users, or even multiple parking ticket spending. The parking scenario is selected from [2] for privacy analysis. Organisations have to dedicate resources to analyse their processes, such as a dedicated team, or they have to buy the service. There are no set frameworks or procedures for companies to follow when analysing the business processes privacy.

The method applied to the smart parking scenario was applied to Autonomous Vehicle (AV) systems by Bakhtina et al. in [3]. Tools used in this thesis are the DPO Tool[1], which analyses compliance with the requirements given by the General Data Protection Regulation (GDPR) [4] and the Pleak tool[2], which analyses data leakage in processes which use privacy-enhancing technologies. The main research question (**MRQ**) is: **How can the DPO and Pleak tools help analyse the parking process compliance with the GDPR?** This question is broken down into sub-research-questions (SRQ):

**SRQ1 - What requirements do organisations need to meet regarding business processes?** The GDPR is used to determine which privacy-preserving measures should be applied to business processes. In addition, the DPO Tool and Pleak Tool relation to the privacy analysis is provided.

**SRQ2 - How does the DPO tool support privacy analysis and show compliance?** The information gathered in SRQ1 is used to analyse the compliance of the smart parking scenario. We use tools from [3] and re-apply the method on the parking scenario from [2]. After the analysis, the processes are complemented with the missing privacy-preserving measures.

**SRQ3 - How does the Pleak tool help select the privacy-enhancing technology?** The GDPR compliant models from answering SRQ2 will be enhanced with additional

[1]DPO Tool can be accessed at `https://dpotool.cs.ut.ee/`

[2]Pleak tool can be accessed at `https://pleak.io/home`

technologies such as Public Key Infrastructure (PKI) and Multi-Party Computation (MPC) and then analysed with the Pleak Tool.

The first step is to use the As-Is business process models as input for the DPO tool. This helps us identify the non-compliance issues followed by the process redesign. The next step is to apply any chosen privacy-enhancing technology and analyse the compliance again. Finally, the Pleak tool is used to analyse the different PETs and their effectiveness in preserving personal data.

As a result, the contribution to the business process of GDPR compliance analysis is as follows:

1. The thesis provides a tool-supported analysis of smart parking, demonstrating the use of the selected tools in adding privacy-preserving measures to business processes. The method used can benefit organisations by helping them understand, how specialised tools can assist them with privacy analysis.

2. The smart parking business processes are enhanced with privacy-enhancing technologies and are redesigned to meet the regulations given by the GDPR. This benefits the system developers as we provide an analysis of the smart parking processes along with the redesigned processes which helps to apply the method on concrete systems.

3. The method used gains extra validation on a different business process from the one provided in [3]. It is possible to generalise the use of the method to more than one business field.

The rest of the thesis is structured as follows. Chapter 2 presents the principles and regulations organisations must meet and the methods that help achieve them. In addition, privacy-enhancing technologies (PETs) are introduced. Next, the smart parking business processes are explained to give an overview of the system to be analysed. Finally, the tools that will be used in the privacy analysis are described. Chapter 3 describes complementing the business process models with privacy-preserving measures. The chapter begins with privacyless model analysis and the addition of data objects. Next, the DPO tool is used to analyse the models' compliance with the GDPR without using any particular privacy-enhancing technologies. In Chapter 4, the privacy-enhancing technologies (PKI and MPC) are applied to the models and another analysis is conducted using the DPO Tool to verify the implementation of the PETs. The chapter ends with the Pleak tool analysis to detect data leakages in the processes. Finally, Chapter 5 concludes the thesis by answering the research questions, providing the limitations of the work and defining possibilities for future work.

# 2 Background

Many processes today are data-driven. A lot of personal data is transferred between different counterparts, exposing the data to threats such as data theft or data manipulation. The General Data Protection Regulation (GDPR), which is the data regulation in the European Union (EU), has gained power over the years, leading organisations to be more aware of gaps in their business processes. This chapter gives an overview of regulations and requirements for processing personal data. Furthermore, tools will be introduced, which are used to analyse compliance with the GDPR and to detect GDPR requirements which are not met. We aim to answer **SRQ1 - What requirements do organisations need to meet regarding business processes?** This question can be split into multiple subquestions:

1. Which principles do the systems that process personal data have to follow?
2. What requirements are given for data processing by the GDPR?
3. What are the requirements for the Smart parking business processes?

## 2.1 Privacy Principles and Regulations

This subsection describes the principles that privacy-preserving systems have to apply to their design. The corresponding articles from the GDPR are reviewed which gives the basis for redesigning the business processes to comply with the GDPR.

### 2.1.1 Privacy Principles

According to the GDPR [4], any data, that can be used to identify a natural person (i.e. data subject), is classified as **personal data**. This data may consist of references to an identifier such as name, an identification number, location or to one or more physical, physiological, genetic, mental, economic, cultural, or social factors which allow to identify the natural person. This means that this data should be private and also secure. The **data subject** is the user or counterpart providing the personal data to the system.

Personal data is a component of information flows between system actors. The information flow is regulated by **data governance** [5] - a system of principles - determining how the data is processed. Since privacy can be defined differently depending on the environment, there has to be a clear identification of actors, the type of data in the flow and the principles used to process the data. This principle is **privacy by design** according to [6], which requires the system to comply with the fundamental privacy principles.

The service provider should help the user present the personal data they want. The actors should minimise the amount of personal data transferred between the system's actors according to GDPR Article 5 c [4]. It is called the **data minimization** principle,

which means that the processing of personal data should be specified, explicit and legitimate [7]. This limits the risks of misusing data and helps the user make easier choices in which information they need to share. The user should be able to control the settings and permissions of their data. Furthermore, the system should also be designed to control which information is exposed and in what way.

**Purpose limitation** is another principle in data processing that suggests that personal data processing should have specific, explicit, and legitimate purposes. This principle determines which data can be collected and processed, what can be done with the data, and the storing period of the personal data [6]. This is somewhat related to the **storage limitation** principle. The storage period of the personal data for processing should correspond to the time period necessary to fulfil the purpose. Personal data should be deleted or anonymized spontaneously and not at the data subject's request.

**Anonymization** of data is a way of processing personal data, resulting in data that cannot be identified to a natural person. According to [6], it is hard to determine whether the data is anonymized, since large amounts of information are available to third parties in different systems. This makes it difficult to verify the anonymization of the data. Another related principle is data **pseudonymization**, which is different from anonymization. According to the GDPR Article 4 (5), "*pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately"* [4].

The systems should process data securely and prevent unauthorised and illegal use of personal data. Secure data processing follows **confidentiality, integrity** and **availability** (the CIA triad) principles. Confidentiality means that the data should be kept from unauthorised access. Integrity is related to confidentiality, referring to the data being trustworthy and complete, and the data should not be modified by any unauthorised party. Lastly, availability means, that the data is accessible whenever needed.

The data subject should know how their data is processed. This is **transparency** in data processing, which implies that certain information is provided to the data subject in an easily accessible way [6]. It is an important trust factor between users and the system and it provides some control over their data.

### 2.1.2 Regulations for Processing Data

The GDPR provides a set of requirements for organisations to fulfil the aforementioned privacy principles in data processing. We will look at some requirements since the compliance analysis does not cover the whole GDPR but only the base requirements needed for processes to reduce privacy problems. In addition to the **data subject**, the system usually has a **controller** and **processor**. GDPR defines the **controller** as a natural or legal person, authority, agency or other body which, alone or jointly with others, determines the purposes of the processing of personal data. The **processor** deals with

processing the data.

Article 7 of the GDPR states the conditions for the consent is strongly related to all of the abovementioned principles. Data subject gives consent to the processing of their data which means that they agree with all the terms given by the processing party and these terms should reflect the fulfilment of the privacy principles. Articles 13 and 14 describe the information provided via **privacy policy**, the preceding step before the data subject consents.

The **controller** shall record all processing activities under the system's responsibility according to Article 30. The record should have the controller information, the purpose of processing, recipients of the data (for example transfers to a third party), the information about the storage period of the data and the description of the security measures. Article 25 of the GDPR refers directly to the **privacy by design** principle, meaning that organisations are expected to implement appropriate measures to ensure the secure processing of personal data and that the processing follows all the privacy principles.

Article 32 describes the security of personal data, which provides the need for privacy-enhancing technologies. The risks must be assessed and an appropriate level of security must be provided. The processing of personal data must be able to ensure the ongoing **CIA triad** application, the **pseudonymisation** and **encryption** of personal data, and the ability to restore the availability in the event of an incident. The system should be regularly tested to evaluate the effectiveness of applied measures.

## 2.2 Privacy Enhancing Technologies

This section overviews possible privacy-enhancing technologies (PETs) used to prevent personal data leakage. Knockaert et al. have described six different types of PETs in [6]:

1. **Privacy-Enhancing Digital Signatures**. A person or a group uses signatures to authenticate in different scenarios. The signatures should not be linkable to a concrete person.

2. **Privacy-Enhancing Authentication**. These techniques allow users to join services without revealing their identity and providing personal data to the system. Even though some of these systems prevent unlinkability, the systems should provide protection against malicious users.

3. **Privacy-Enhancing Communication Systems**. These technologies focus on the secure transfer of the data via communication networks.

4. **Privacy-Enhancing Encryption Technologies**. The encrypted data can only be decrypted by an entity with the specific set of attributes needed for decryption.

5. **Privacy-Enhancing Computations**. These technologies enable secure computing on their inputs while they are kept private. This means that each party does not have more knowledge of the data than they are provided with.

6. **General Anonymization Technologies**. Technologies, that anonymize data after processing.

The following PETs are chosen to be used in the thesis to secure the personal data moved between different counterparts.

### 2.2.1 Public Key Infrastructure

The public key infrastructure (PKI) uses a system consisting of two keys - one for encryption, meaning that one key is used to secure the data, and one for decryption, which is used to convert the data to a readable form again. It is important to note that the encryption key is public because the decryption key cannot be determined using the encryption key. This pair is called the public and the private key pair. Since the encryption key is public, the party, to whom the key belongs, can receive encrypted messages. They have the knowledge of their private key, which can be used to decrypt the messages. This way, the transportation of information is safe, since the information is not moved in plain text for example [8].

### 2.2.2 Multi-Party Computation

The main idea of Multi-Party Computation (MPC) is that data is split into pieces. In this paper's context, the data is split and stored in different places and it is possible for some authorised party to gain access and reconstruct this data to make sense of it. The data is split into pieces in a way that removes the possibility of making sense of one piece without the others. Furthermore, the data is kept private from the storing parties and these roles can cooperate to compute the original data [9].

## 2.3 Privacy Analysis Tools

The main tools for checking compliance with the GDPR used in this research are DPO Tool[3] and Pleak Tool[4]. The first tool can be used to analyse different business processes and assess their compliance with GDPR. The second tool, Pleak, can be used to analyse the selected PETs to prevent data leakages. Both tools use **Business Process Model Notation (BPMN)** [10] models as input, which is the language to design graphical views of business processes.

[3]DPO Tool can be accessed at `https://dpotool.cs.ut.ee/`

[4]Pleak tool can be accessed at `https://pleak.io/home`

Manual analysis or the use of specialised tools can be applied to assess the privacy of a business process. Various commercial GDPR compliance checkers are found on the Internet (e.g., secureprivacy[5], Didomi[6]). In addition, there are specialised companies which provide services for web solutions in order to check compliance with the regulation. The aforementioned tools are applicable to already deployed applications which means they are not usable for systems in the early stages or which are not web-based. This means that these tools are not to be analysed in this research.

The following tools are used to assess compliance with the GDPR and the security of business processes used in the modern Smart Parking systems described before. These tools are chosen to validate the tools further and recommend changes. It is a further development to the work in [3] with a new scenario to see the performance and support provided by the tools.

### 2.3.1 DPO Tool

DPO Tool[7] is a prototype which uses business process models and GDPR model [11] to help achieve compliance with the regulations. The main function is to compare the BPMN model of the assessed process with the GDPR model. This tool requires a BPMN diagram that demonstrates the flow of the process to be assessed.

The following instructions should be observed to conduct a tool-supported analysis using the DPO tool. Firstly, the As-Is business process model should be uploaded to the tool for evaluation. After this step, the user should define the main GDPR model elements (e.g., data subject, controller, processor and personal data). The next step consists of the comparison of the provided model with the GDPR model. This results in a GDPR model highlighting the non-compliance issues. If these issues exist, the owner of the process should complement the existing model with regulation-compliant features. Finally, the improved business process model can be used in further compliance control processes.

There are a couple of advantages to using the DPO tool. It is an open-source tool that enables everyone to have free access and usage even though it is in the prototyping stage. Furthermore, the tool can be used throughout the whole lifecycle of a system since the only requirement for the analysis is the BPMN model and not the fully developed system compared to the commercial tools, which require a deployed application. Lastly, Sing [12] provides a comparison of manual regulation compliance achievement with the tool-supported analysis which demonstrates that the tool is capable of identifying issues which remain unfound during the manual compliance analysis.

The tool presents a few disadvantages as well. While comparing the business process with the regulations, the national adaptions of GDPR by the EU Member States are not

[5] `https://secureprivacy.ai/`

[6] `https://www.didomi.io/gdpr`,

[7] DPO Tool can be accessed at `https://dpotool.cs.ut.ee/`

taken into account. Another problem regarding the requirements is that they can not all be modelled, which means that the model covers less than half (40 out of 90) articles.

### 2.3.2 Pleak Tool

Pleak (Privacy Leakage)[8] is an open-source application prototype which is used to uncover possible data leakages in business processes. It is beneficial for processes which include data processing and communication between multiple counterparts by finding possible data leakages and the extent and by whom the data is leaked. Pleak tool assists in evaluating the effect of PETs used in business processes.

The tool uses privacy-enhanced BPMN (PE-BPMN) [13] as an input. As a result, Pleak provides multiple analysis reports of different levels. These reports contain information regarding the data flows and actors who receive the data and the extent of the received data. These reports can be used to identify suitable PETs for the system and their effectiveness on preventing data leakages in the whole process.

## 2.4 Related Work

Pullonen et al. [13] have suggested that **Privacy-Enhanced Business Process Models (PE-BPMN)** can be used to depict the use of privacy-enhancing technologies in business processes and to analyse the flow of private information. Another reason for this modelling is the convenience of representing the processes to different stakeholders and organisations. Stakeholders become more aware of potential security risks, and these models can help with the communication between different counterparts.

Bakhtina et al. have introduced a tool-supported method for business process analysis in [3]. In this thesis, this method is applied to a scenario different from the scenario analysed in the aforementioned paper. The paper focuses on Autonomous Vehicle systems and their interaction with the passenger. We apply the steps described by the method to a new scenario, which gives extra validation for the method and the ability to generalise the usage of the method on different systems and their processes.

The parking process and its privacy issues have been described by Knockaert et al. in [6]. Only the parking request sub-process is analysed and redesigned to comply with the GDPR while in this thesis, we cover the full smart parking process starting from registering the user up to the parking time extension and finishing the parking. In addition, only PKI is applied to the process, and no other method is used to evaluate the PET's effectiveness. We use the parking scenario and expand the method on multiple processes from the smart parking system. We go into more detail when analysing the different sub-processes. The process models are redesigned to use multiple different PETs, and their effectiveness is analysed using the Pleak tool.

[8] Pleak tool can be accessed at `https://pleak.io/home`

## 2.5 Smart Parking Business Processes

The system under evaluation is the smart parking system. The business processes that depict smart parking system operation are described in [2]. They are reconstructed using a BPMN editor[9] to be able to use the possible tools to evaluate the fulfilment of privacy requirements of the system.

There are three main actors in the system, additionally there is a trusted third-party actor that plays a role in payment management and registering user. It is also assumed that communication between the actors is secured. The data provider is the **User Device**, which represents the user and its main function is to store and present permits and cryptographic keys. It communicates with the **Parking Service Provider (PSP)** to exchange information with the **Parking Lot Terminal (PLT)**. The PSP is responsible for registering the user when the service is first used. It also generates cryptographic parameters and keys in the parking process. It is assumed, that the PSP is a semi-trusted party. Finally, the Parking Lot Terminal (PLT) is responsible for generating parking permits, handling the payment and allowing to enter the parking lot. Furthermore, if the user requests an extension, the PLT handles these requests and generates a new permit for the user.

There are **5 sub-processes** regarding the parking system (see Fig. 1):

- First, during the **Register User** sub-process, the user uses their device to provide a PSP with the details of their digital identity. Using these details, the PSP registers the user and provides them with the credentials and a secret key which are stored in the user's device.

- Then, during the **Issue Parking Permit** process, the user creates a parking request which is sent through the PSP to the PLT. Following the request, a user performs the payment which is sent through the PSP to PLT. The PLT processes the request and the payment information and generates a parking permit for the user. The permit is sent through the PSP to the user device and the PLT stores this transaction information.

- The next sub-process is the **Park Vehicle**, during which the user authenticates to the system and the PLT processes the user credentials. After the confirmation, the user sends their parking permit for verification. The user is then notified of the status of their parking permit. When the permit is valid, the user is allowed to enter the parking lot, otherwise, a new permit generation process is started.

- The fourth sub-process is the **Request Parking Extension**, where the user sends an extension request through the PSP to the PLT. The PLT then tries to find a relevant parking permit and notifies the user about the validity of the permit. If the

[9] `https://demo.bpmn.io/new`

permit is invalid, the permit generation process is started, otherwise, the user is granted a parking time extension.

- Finally, the sub-process of **Analyse Statistical Data** has an utilitary role in recording the key steps within the parking scenario needed for further analysis of the scenario performance.

All the sub-processes are analysed but the main text of the thesis focuses on the two sub-processes - Issue Parking Permit and Analyse Statistical Data - which are described in more detail.

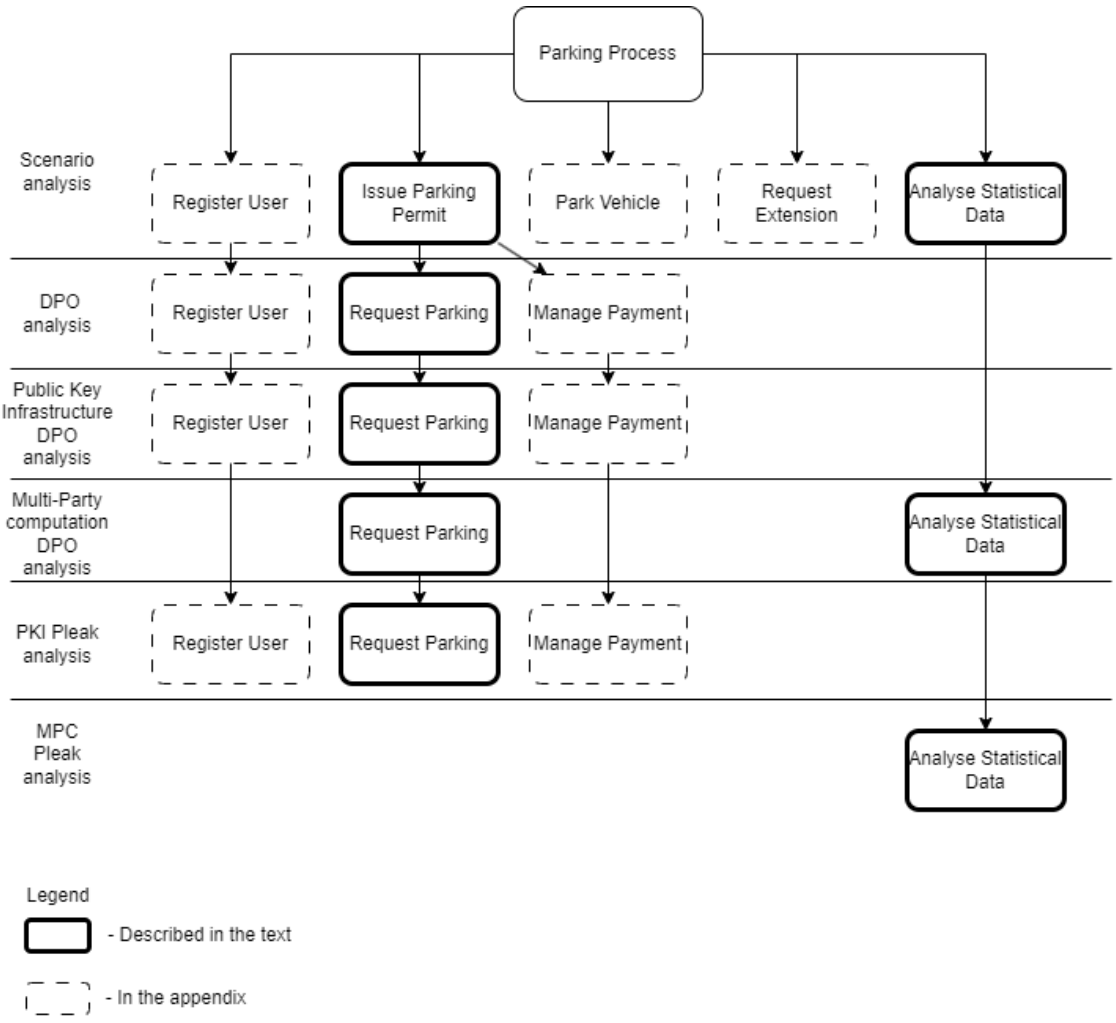


Figure 1. Privacy analysis steps

### 2.5.1 Description of Parking Request

The sub-process for issuing the parking permit is described more thoroughly (see Fig. 2). A **ParkingRequest** is first sent and transferred for processing for the permit. The request contains **personal data** like user credentials, location, and vehicle information. As seen from the diagram below, the user is not provided with a privacy policy, which contains information about the processing of personal data. Furthermore, the user does not provide consent to data processing to the system. This means that the process violates the requirements provided by the GDPR. After the request, the user makes the payment, and the information is sent for processing to PLT. The **payment information** is considered personal data, since it contains card information, thus needing protection in the process. Similarly to the request data object, the user has not been provided with the processing information and has not had the opportunity to consent to these terms. Having the information from the request and payment, a permit is generated and sent back to the user device. As seen from the diagram, the processor does not follow the **privacy by design** requirements and the processing is unsecured. Furthermore, the processing of the data is not recorded in any manner, which means the record is missing, which provides information about the completed processing of personal data. Finally, the parking lot saves this transaction. Appendix II contains other detailed sub-process models.

### 2.5.2 Description of Analysing Statistical Data

Another scenario to be analysed is related to logging the whole parking process. The main idea for this sub-process is to log each processing task, which can be analysed later. Fig. 3 contains a simplified model of the sub-process. Parts of all four sub-processes mentioned before are included. The PSP has a smaller role when the model is not enhanced with PETs - mainly just registering the user and transferring some data. The vulnerable data in this scenario is the **ParkingLog**, which holds the processing information from different tasks. As seen from the diagram, the log is not stored in a secure way, meaning that the PSP stores the whole log as plain information and the data is stored in one storage. This can cause major security issues; since the data is in plain text, it is easy to read, and the logs are stored as one piece, meaning it is easy to redeem all of the logs at once by malicious activities.

## 2.6 Summary

In this chapter, we reviewed the privacy principles for designing privacy-preserving systems, the requirements provided by the GDPR for companies to follow and fulfil these principles and the smart parking scenario and its requirements to answer the **SRQ1** "What requirements do organisations need to meet regarding business processes?". For convenience, this question was split into three sub-questions.

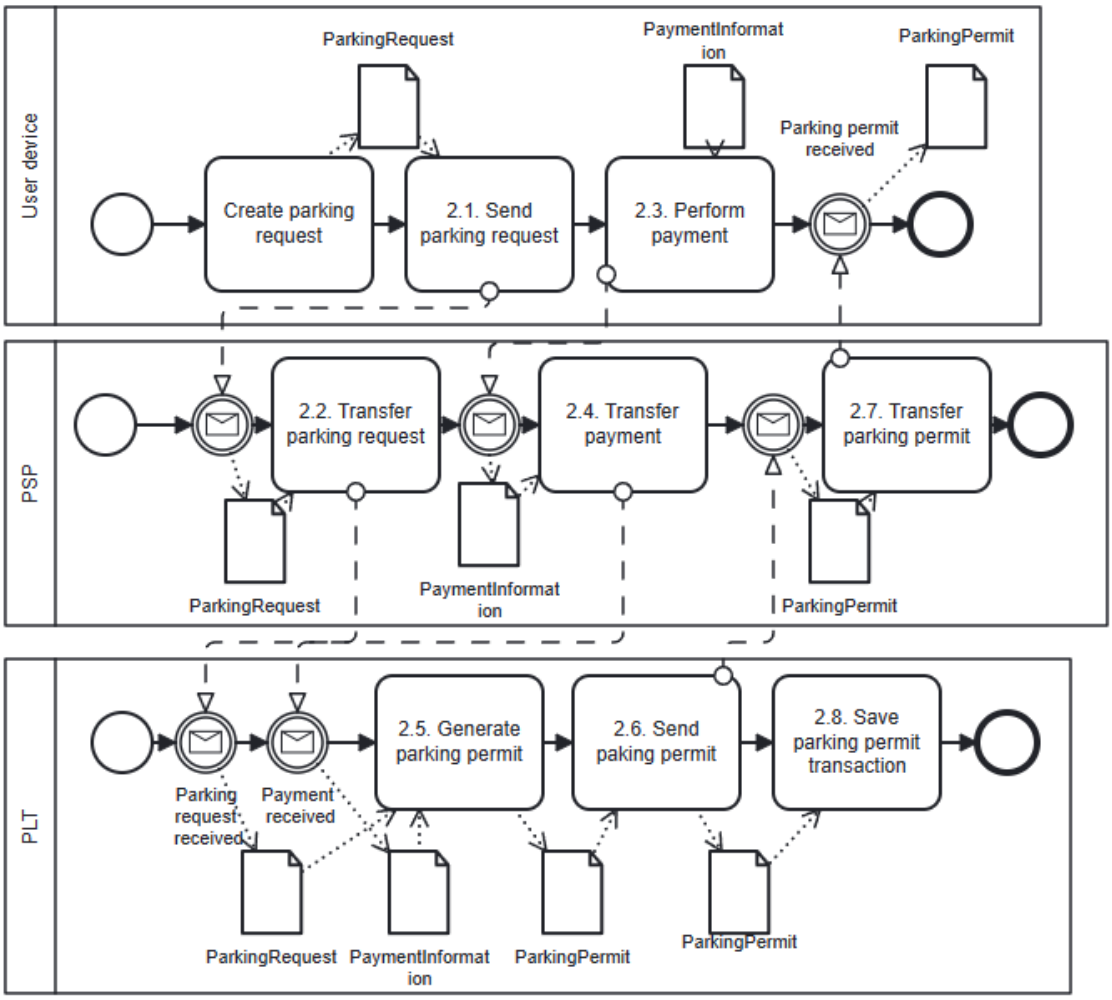


Figure 2. Issue Parking Permit

**Which principles do the systems, that process personal data, have to follow?** We reviewed the privacy principles described in [6] and provided a set of principles that organisations should follow when designing data processing systems. We defined six principles: privacy by design, data minimization, purpose limitation and storage limitation, anonymization and pseudonymization, secure processing (CIA triad), and transparency.

**What requirements are given for data processing by the GDPR?** We reviewed the GDPR and the requirements that are in the scope of this thesis. A number of articles correspond to various principles provided in the answer above. The data subject has to be provided with a Privacy Policy, which is related to the transparency principle, and it should describe the processing of the personal data. Before processing any data, the user has to give their **Consent** to the processing, which has to be freely given and also

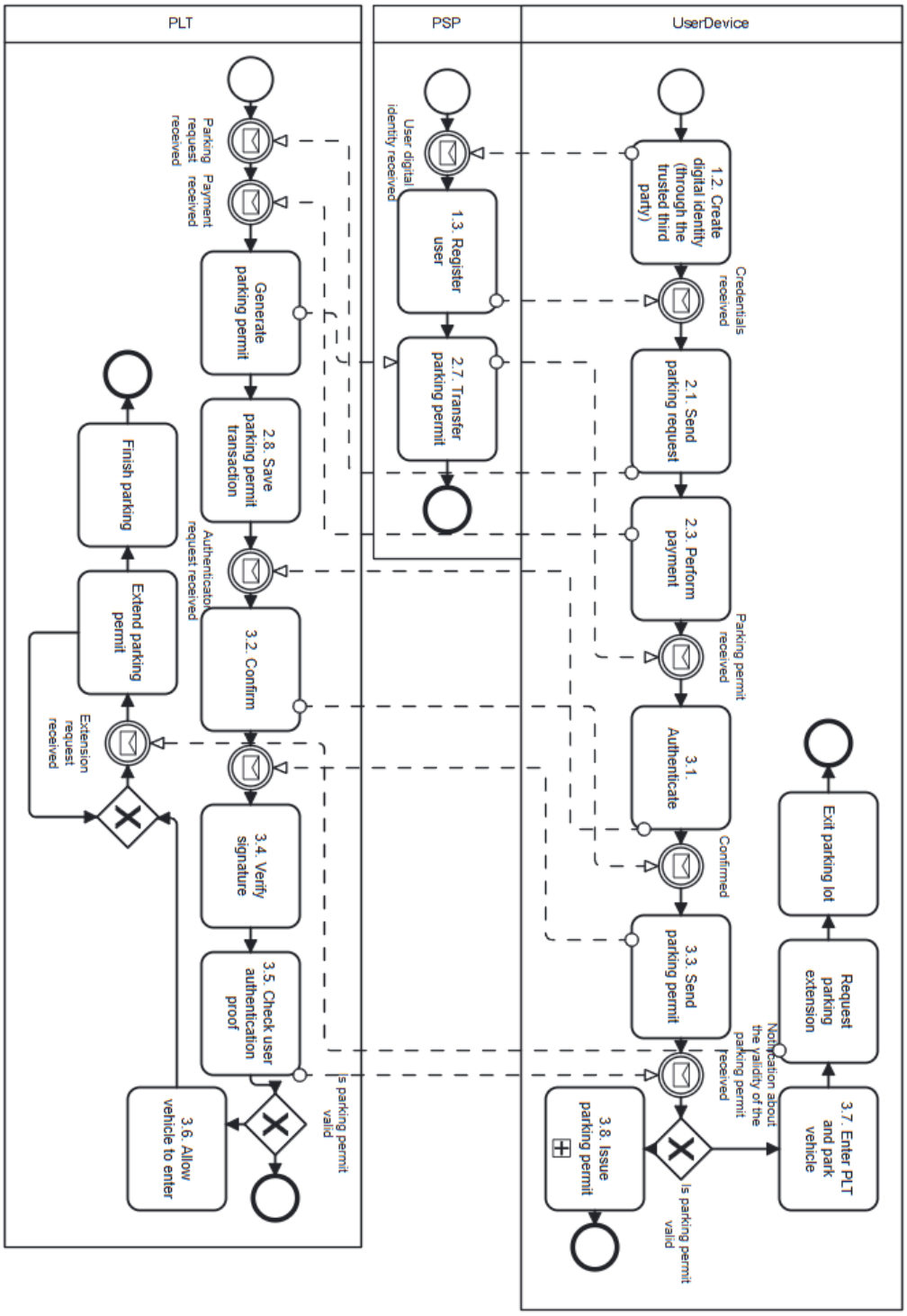


Figure 3. Process for Statistical Analysis

withdrawable when the user does not wish their data to be processed any more. The GDPR also gives requirements for the system which correspond to a number of principles. The processing system has to follow the **Privacy by Design** principle, minimise the data used, limit the storage period and process the data only for the reasons given in the Privacy Policy. The personal data has to be processed in a way that the natural person is not identifiable at least without some extra parameters after the processing. The processing has to be secure and PETs can be used to enhance the systems. The processing of the data has to be recorded as well, and the record should include information about recipients, processing system, and storage period.

**What are the requirements from the Smart parking business processes?** We reviewed the smart parking business processes that were used for analysis in the thesis. A preliminary analysis of the processes was also conducted to detect privacy issues. The data objects were identified, which we have to protect during the processing of the data which are DigitalIdentity and PaymentInformation. In addition to being protected from malicious activities, the data should not be visible to the PSP, who is a semi-trusted actor and who mostly handles the transportation of the data between the user and PLT. The user does not have an overview of the process and what is done to their data. Furthermore, the user does not have the opportunity to give their consent to the processing of their personal data, which violates the requirements set by the GDPR. The system does not follow the secure processing principles, and the processing is not recorded, which means that there is no overview of the processing done.

# 3 GDPR Compliance Analysis with DPO Tool

In this chapter, the sub-process models from Chapter 2 are analysed using the DPO tool[10] to identify the exact issues with compliance with the GDPR. The sub-processes are then redesigned according to the feedback from the tool and the analysis is run once again to verify the changes. We answer **SRQ2 - How does the DPO tool support privacy analysis and show compliance?** At this stage, the BPMN models are not designed to depict the use of PETs.

## 3.1 Analysis of Request Parking Sub-Process

In Chapter 2, we described the personal data objects that we have to protect in the Issue Parking Permit process. Since the process contains two different data objects, that need protection, the process must be split into two sub-processes to be able to analyse the privacy of each of the data objects within the sub-process: **Request Parking** and **Payment Management**. We remove the tasks related to payment management from the sub-process model (see Fig. 4), which leaves the **ParkingRequest** data object as the only personal data object that needs protection. The privacy issues described in Chapter 2 remain. Register User and Manage Payment sub-process models used for analysis are in Appendix III.

### 3.1.1 Request Parking Sub-Process Compliance with GDPR

The aforementioned sub-process models are given as input to the DPO Tool. For the first analysis, we must identify the personal data object, which is the **DigitalIdentity**. Next, the counterparts' roles in the system must be set. In the Request Parking case, the User Device is identified as the **Data Subject**. The PSP transfers the data and is identified as the **Controller** and the PLT is responsible for processing the data and is identified as the **Processor**. In addition, the processing task has to be identified, which in the Request Parking sub-process is **2.5 Generate parking permit**. These fields are mandatory to fill in the first analysis and other fields can be left to their default values. The exact inputs for the Request Parking sub-process analysis can be seen in Table 1.

### 3.1.2 Output of DPO Tool

As a result, the DPO Tools provides a compliance analysis which gives an overview of the issues in the process (see Fig. 5). The process is missing the privacy policy, which should contain information about the processing of the data and the data subjects' rights to the data. The consent form is also missing, which should be given by the user to the system to process the personal data provided lawfully. We can see that the system is

[10]DPO Tool can be accessed at `https://dpotool.cs.ut.ee/`

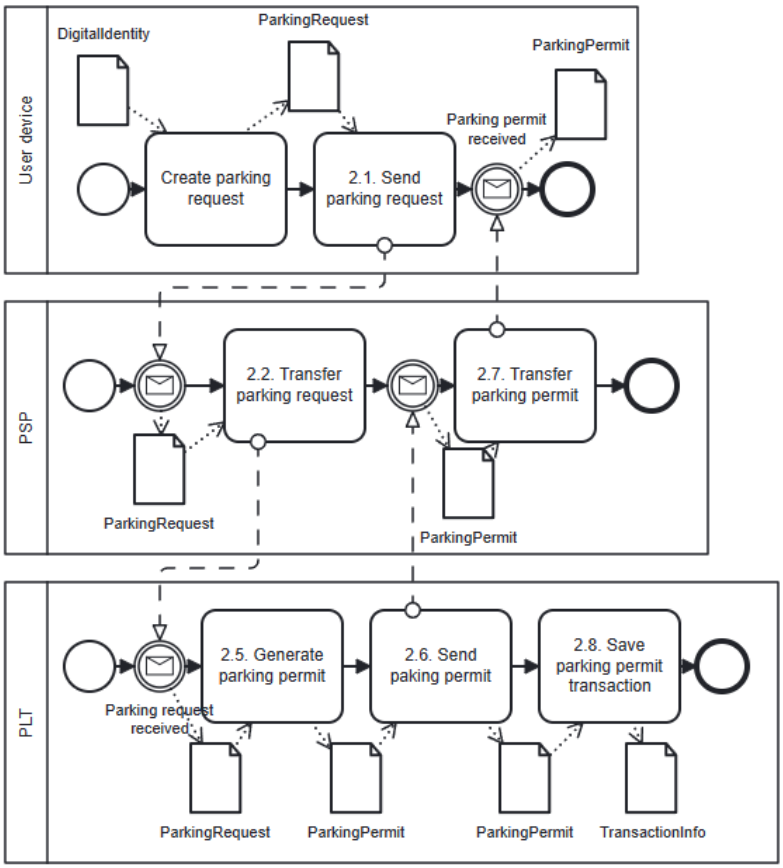


Figure 4. Request Parking Sub-Process

Table 1. DPO Tool Inputs for Request Parking Sub-Process

| **Sub-Process** | **Data subject** | **Controller** | **Processor** | **Processing task** | **Personal Data object** |
|---|---|---|---|---|---|
| Request Parking | User Device | PSP | PLT | Process Parking Request | DigitalIdentity |

missing the attributes related to the privacy-preserving design of the processing system. This means that the processing of personal data does not follow the privacy principles reviewed in Chapter 2 and introduces threats and leakages to the system. Furthermore, the processing task is not being recorded, leading to the record of processing being missing. There is no overview of the processing activities, who receives the processed data and the period of storage. Lastly, we can see that the system does not apply any security measures (PETs) which violate the requirements provided by the GDPR.

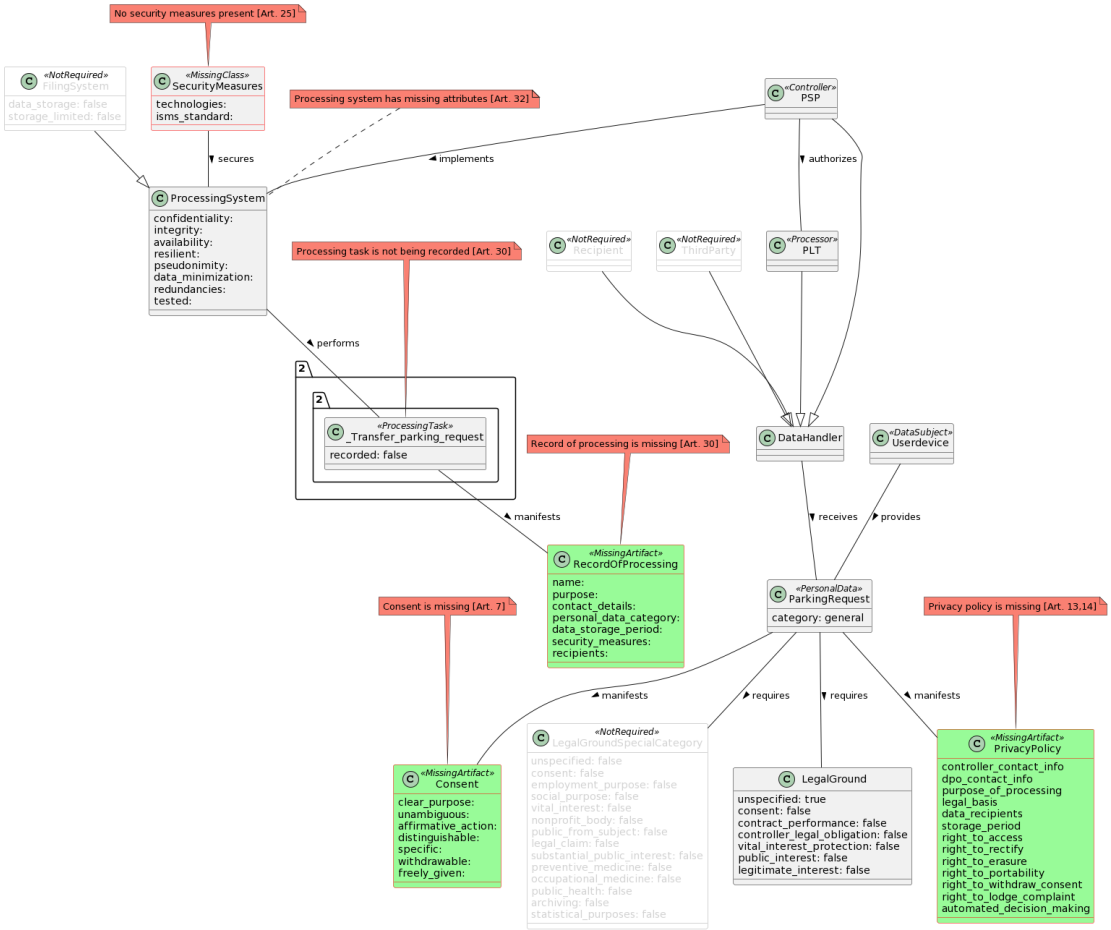


Figure 5. Non-compliant Request Parking DPO Tool Output

## 3.2 Re-Designing the Request Parking Sub-Process

After the initial analysis and the results from the DPO Tool, we can reconstruct the sub-process models (see Fig. 6). First, we label the different counterparts according to the input used for the first analysis. The User Devices is labelled as **Data Subject**, the PSP is labelled as **Controller** and the PLT is labelled as **Processor**. Furthermore, we label the personal data object as **personal data**, which needs protection, which in the Request Parking case is the **DigitalIdentity**. The processing task, which processes the data given by the user, must be labelled as a processing task, and we add the task Process parking request as a processing task to the system before generating the permit with the processed information.

The next step is to provide the user with the **Privacy Policy** which will be labelled as an **Artifact**. The policy should also have the attributes required by the GDPR which include contact information, purpose of processing, user rights to the data, storage period,

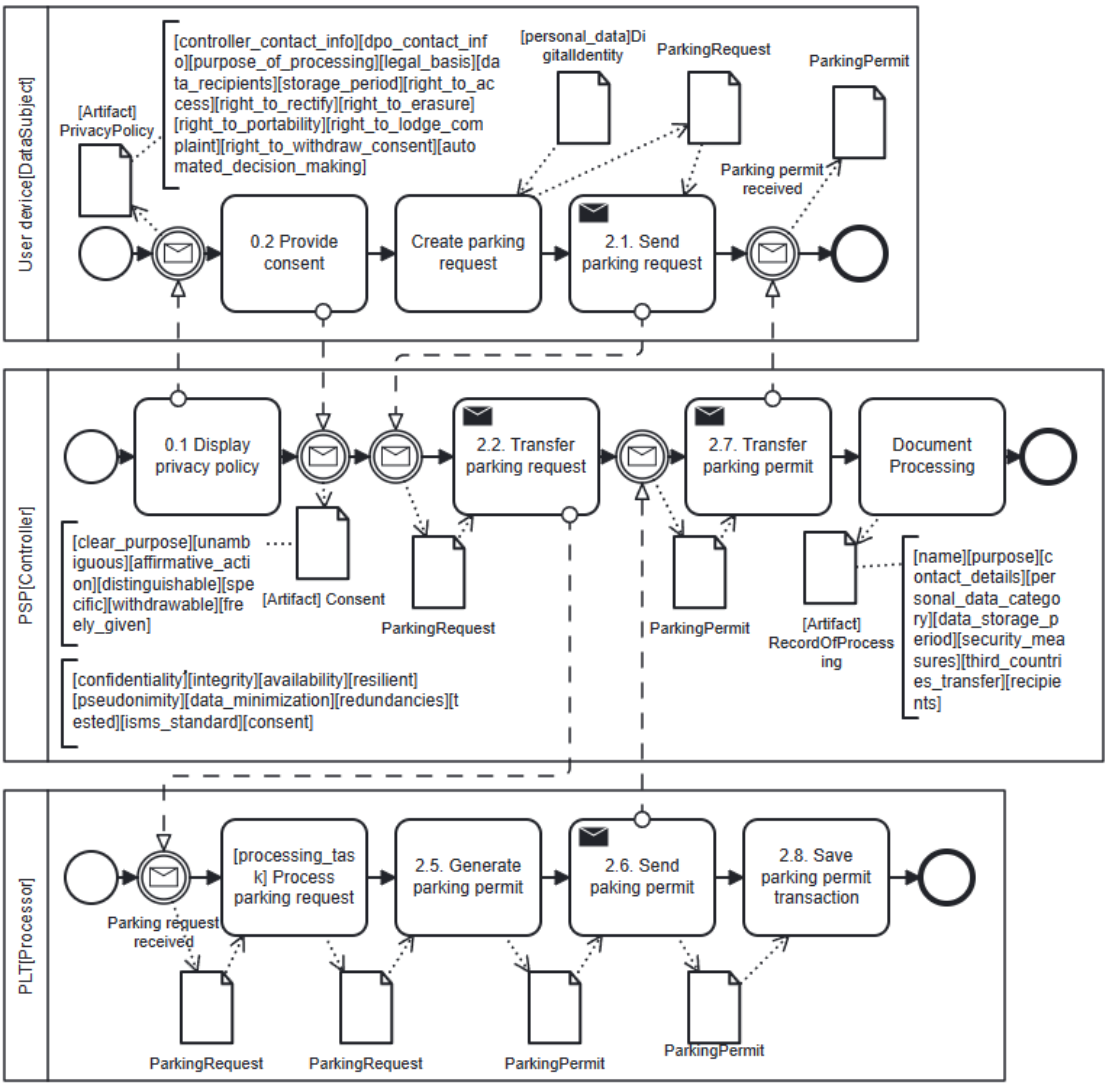


Figure 6. GDPR Compliant Request Parking Sub-Process

recipients and the legal basis. A task **Display Privacy Policy** is added and the Controller is responsible for displaying the policy to the Data Subject. Then the task **Provide Consent** is added for the data subject, which allows the Data subject to give their consent to the Controller for processing their personal data while following the Privacy Policy. The Consent object is labelled as an **Artifact** and has the following attributes: clear purpose, unambiguous, affirmative action, distinguishable, specific, withdrawable and freely given. The controller receives this consent and then the original flow of the process begins.

The system must follow the **Privacy-By-Design** requirements, meaning that we must

add the attributes regarding secure processing to the model. This includes the **CIA triad**, **resilience, pseudonymity, data minimization, redundancies, tested, consent and ISMS standard**. ISMS means information security management systems, and this attribute gives the signal, that the process is using a PET, but the technology is not specified. Lastly, the **Artifact** for the Record of processing is generated by a task **Document Processing**, which has to be complemented with attributes required by the GDPR.

After the model has been redesigned, the DPO Tool is used to validate the changes. As a result, we can see that the model follows the requirements given by the GDPR (see Fig. 7). Register User and Manage Payment re-designed sub-process models can be found in Appendix IV.

## 3.3 Summary

In this chapter we analysed the As-Is business process models and their compliance with the GDPR. The DPO Tool was used to support the business process analysis and to identify the GDPR compliance issues within the processes to help answer **SRQ2** - *"How does the DPO tool support privacy analysis and show compliance?"*. The tool displayed the compliance issues which are present in the models. The analysis consisted of missing privacy-preserving measures and corresponding articles from the GDPR which helped to re-design the business processes. In addition, the tool was used to verify changes to the models.

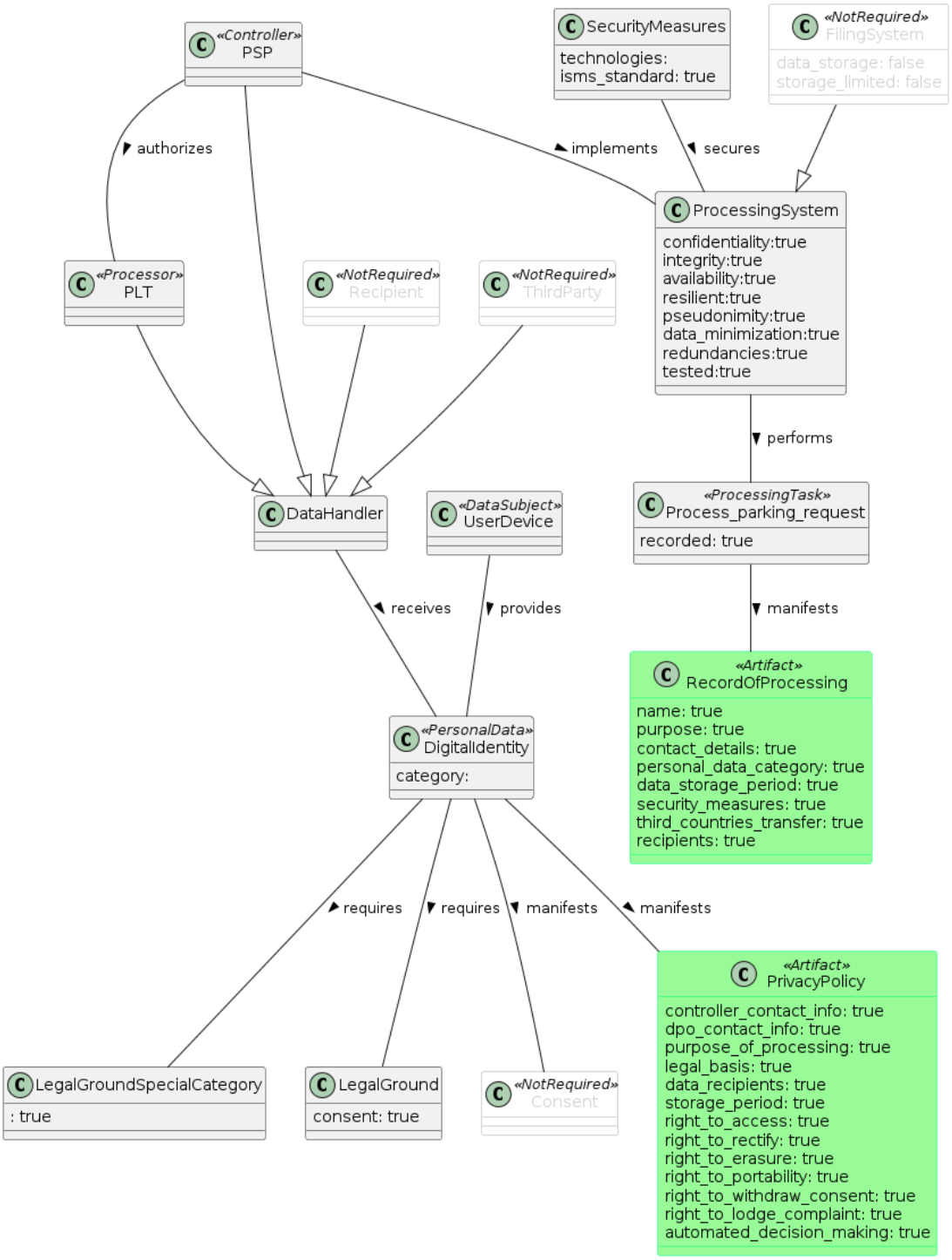


Figure 7. DPO Tool Output for GDPR Compliant Request Parking Process

# 4 Analysis of Privacy-Enhancing Technologies

The GDPR-compliant sub-process models are re-designed in this chapter to integrate the PETs selected in Chapter 2. The PKI and MPC technology are applied in the sub-processes and the re-designed models' compliance with the GDPR is validated using the DPO tool. If the models are correct and compliant with the GDPR, we move to the Pleak tool[11] to analyse the applied PETs and how they can help preserve the privacy of personal data in the smart parking business processes.

## 4.1 Application of Privacy-Enhancing Technologies

The sub-process models in the previous chapter have the attribute **ISMS standard** which means the processes should use some PETs, but the models do not depict the usage of any particular PET. The GDPR compliant sub-process models are re-designed to demonstrate the usage of PKI and MPC technologies. The PKI technology is applied to the **Request Parking**, **Manage Payment** and **Register User** sub-processes. The MPC technology is applied to the **Request Parking** sub-process and to the **Analyse Statistical Data**. When the models are complete, we once again analyse them using the DPO tool to validate compliance with the GDPR and that no syntax errors are present.

### 4.1.1 Request Parking Enhanced with Public Key Infrastructure

The key idea of PKI is to use a public and private key pair to keep personal data secure during data transfers. The processing party holds the private key since it is the one to decrypt the data in order to receive its contents for further processing. The data is decrypted by the counterpart which provides the personal data object. In addition, the channels which are used for data communication must be secured.

The request parking sub-process re-design is described more thoroughly (see Fig. 8). First, the **ParkingRequest** data object, which contains the users personal data, is **encrypted** using a public key from **key pair A**. The **Encrypt parking request** task is added to encrypt the ParkingRequest data using the public key. This results in an encrypted data object, which is sent through secured channels to the processor. Before PLT can generate a parking permit, the ParkingRequest has to be decrypted using the private key from **key pair A**. This is done by adding a separate task to the sub-process model. After the permit is generated, the system should prepare it for transfer back to the user device, which means there is a key pair B that differs from the key pair A. This is because the receivers of the data differ which means each receiver has their own key to decrypt messages. The public key from key pair B is used to encrypt the **ParkingPermit** and is transferred to the user device through secure channels. For the user to make sense of the parking permit data, the private key from key pair B is used to decrypt the **ParkingPermit** data.

[11] Pleak tool can be accessed at `https://pleak.io/home`

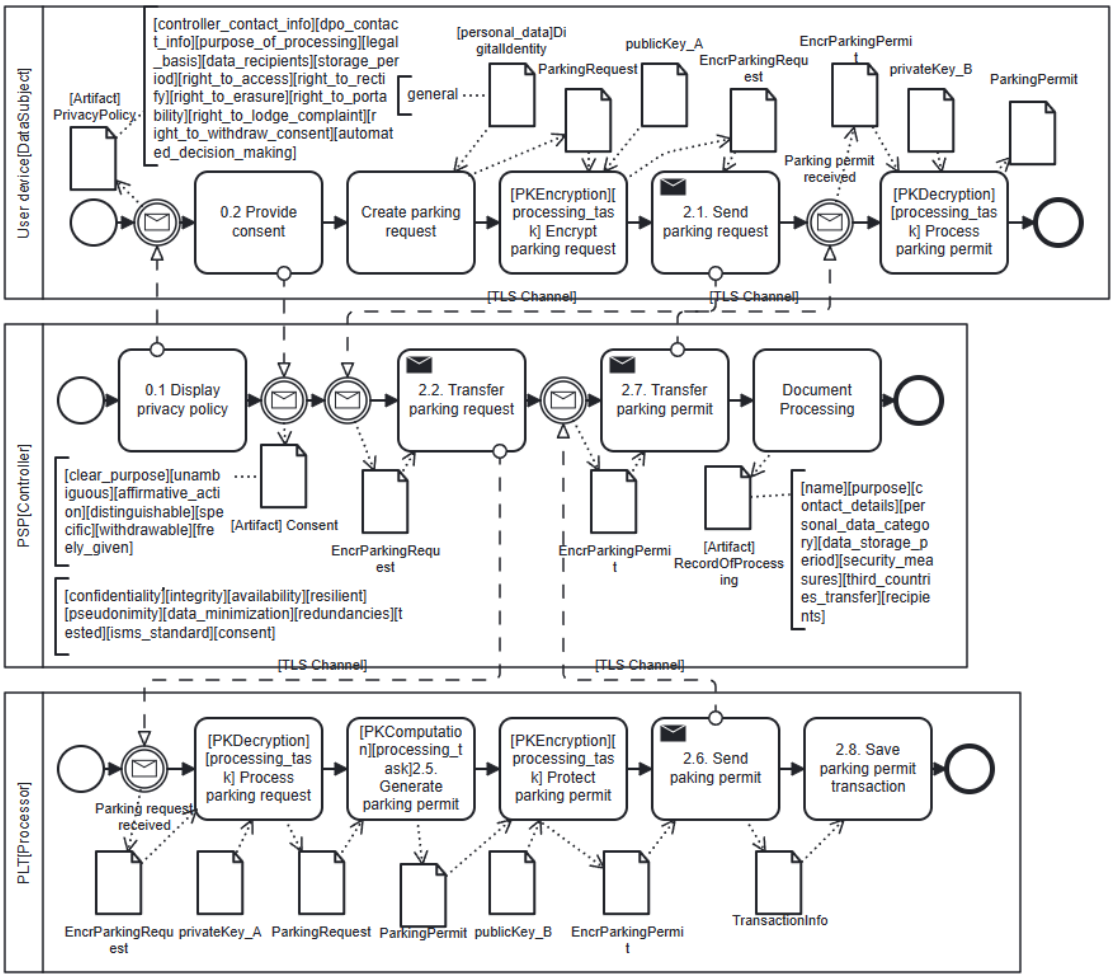


Figure 8. Request Parking Sub-Process Enhanced with PKI

After the model is complemented with the PKI technology, we validate the compliance with the GDPR using the DPO Tool. The DPO analysis result shows, that the model is syntactically correct and follows the regulations (see Fig. 9). The same workflow is applied to the Manage Payment and Register User sub-processes, in which detailed sub-process models are displayed in Appendix V.

### 4.1.2 Request Parking Enhanced with Multi-Party Computation

The key idea of MPC is to introduce a **trusted external party**, which is an external storage apart from the original parts of the process which stores one part of the split data. The key idea of MPC is to **split vulnerable data** into multiple pieces and each piece is processed by a different party. In addition, a trusted external party can be introduced to store a part of the split data or the storage can be selected from the existing parties,

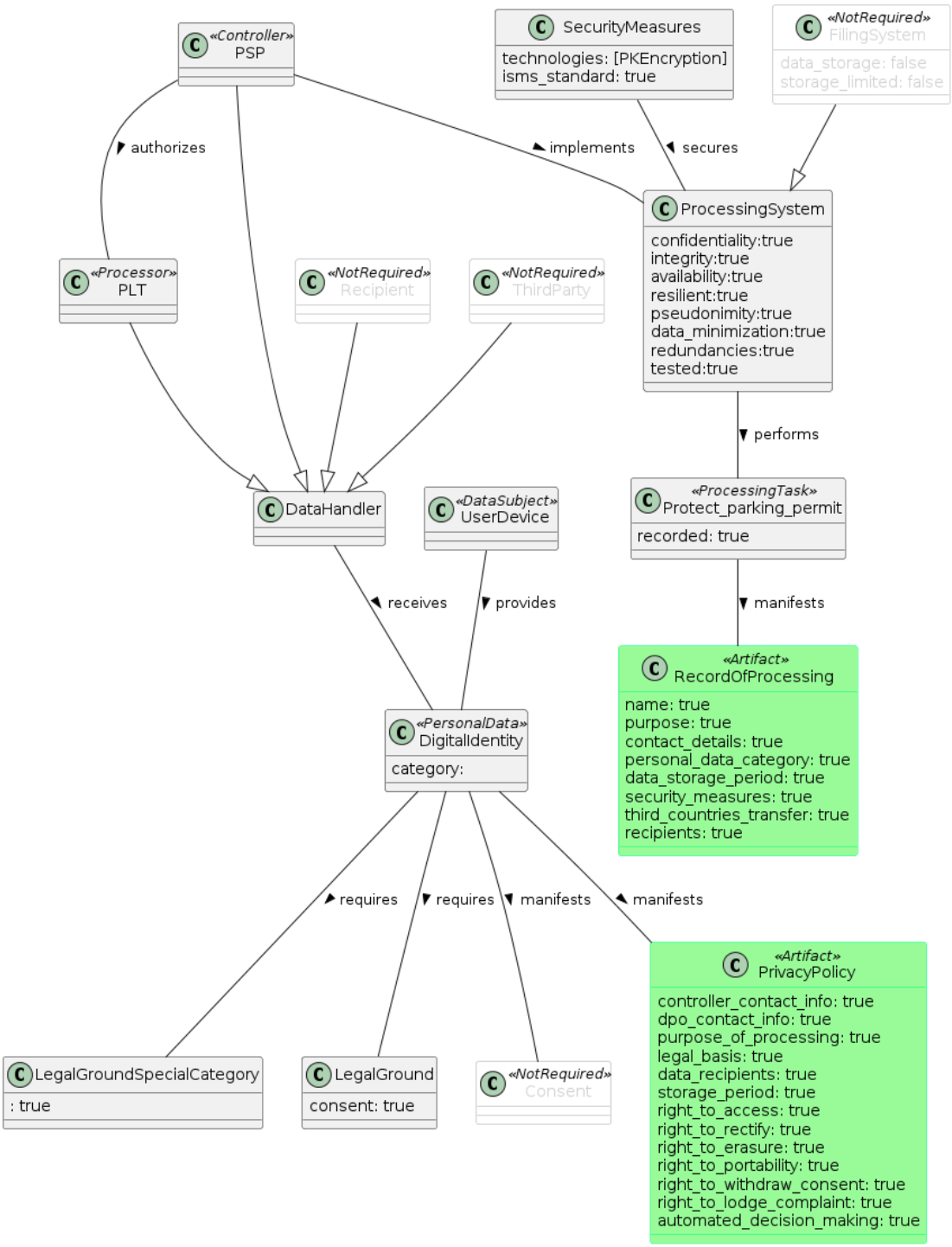


Figure 9. DPO Tool Output for the GDPR Compliant Request Parking with PKI

if there are enough of them. When there is a need to redeem the complete data object, these different processing parties can provide their share of the processed data and the complete data object is then computed using all the information. This way, it is difficult to obtain the complete data object by malicious users or programs because when they attack one part of the system, they cannot receive the complete set of attributes and fields related to the personal data object.

The main change to the Request Parking sub-process model involves the secure split of the personal data object and the introduction of a trusted external server which handles the processing of one part of the personal data object (see Fig. 10).

The ParkingRequest data object is split into two objects, which each contain data from the request; for example, one of the objects could contain the request time and vehicle information, and the other could contain the user details. The first split part is sent to the PLT and the other to the PSP for processing. This results in two parts for the parking permit which should be combined into the complete ParkingPermit data object. During the next sub-process, which is the Park Vehicle Sub-Process, the ParkingPermit is checked as a whole. Thus, MPC will only add protection to the ParkingRequest, but not the ParkingPermit.

### 4.1.3 Analyse Statistical Data with Multi-Party Computation

To demonstrate the use of the MPC technology in the smart parking business processes, we will use the Analyse Statistical Data from Chapter 2. To better understand the Analyse Statistical Data with MPC, the model is split into two sub-processes (see Fig. 11): **Log processing tasks** and **Store Logs**.

The system generates logs after every processing task (see Fig. 12), which are stored in the **ParkingLog** data object, which we will consider as vulnerable data in this process. The ParkingLog contains information about the permit generation, permit verification, entrance to the parking lot, parking time extension and exiting the parking lot. The different counterparts follow the GDPR, which means that the system is secure, the processing is recorded, the user is provided with a privacy policy, and they can give their consent to the processing of their data. The second part of the process is the **Store Logs** sub-process, which applies the principles of the MPC (see Fig. 13). The log generated in the **Log processing tasks** sub-process is split by the PLT into two different data objects. These data objects include different parts of the original data; for example, one contains information about permit generation and verification, and the other data objects contain the entrance, extension and exit information or the data object can be split using an algorithm that does not consider the business value of the log. Since the smart parking scenario states that the PLT does not store any information, the data is sent to the PSP for storing, and the other data object is sent to a trusted External Storage, which we introduce to the system. This results in the split parking logs being stored in different counterparts of the system. In this way, the MPC is correctly applied to the Analyse Statistical Data,

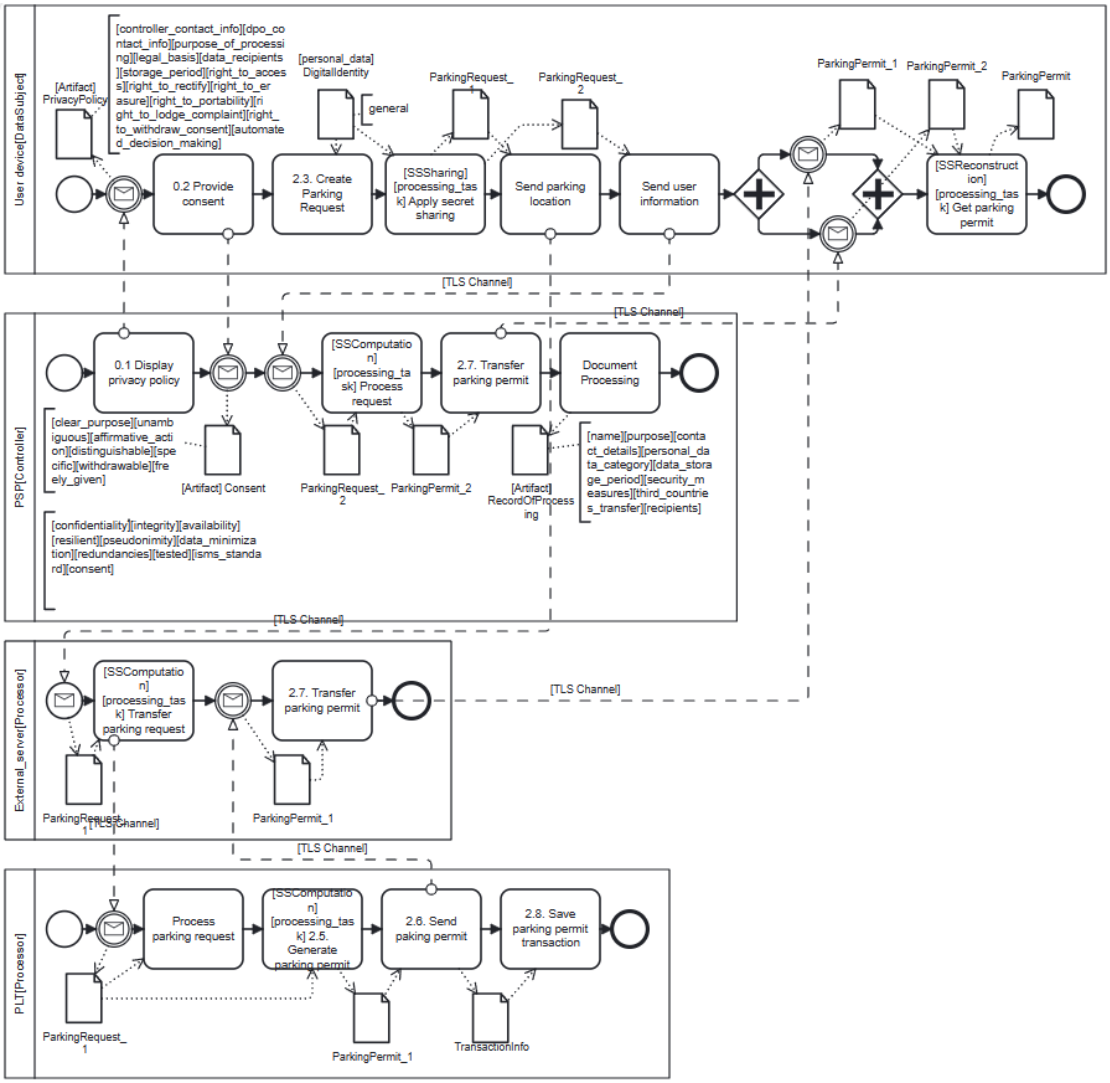


Figure 10. Request Parking MPC Implementation

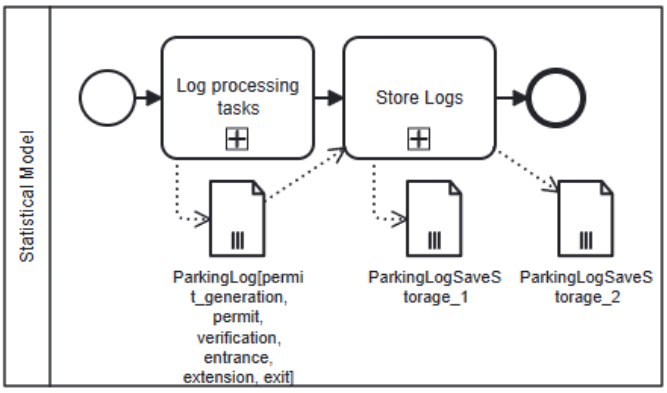


Figure 11. Analyse Statistical Data Sub-processes with Generated Data Objects

and it demonstrates that when an authorised party needs to review the logs, the data has to be retrieved from different storages and computed into a complete log.

## 4.2 Process Analysis with the Pleak Tool

The models depict the use of PETs and are ready to be analysed with the Pleak tool. The tool analyses the efficiency of the selected PETs in keeping the vulnerable data secure throughout the processing. The models are used in **Simple Disclosure analysis** which analyses the visibility of the data objects used in the whole process. As a result, a table containing the data objects and their visibility in different counterparts of the systems is generated.

### 4.2.1 Request Parking Sub-Process Enhanced with PKI

The Request Parking sub-process model, which implements the PKI technology, is converted to an equivalent model in Pleak with a different syntax (see Fig. 14). The labels, data objects and tasks directly related to the PKI are labelled in the PE-BPMN (Privacy Enhanced Business Process Model Notation) and Leaks-When editor to demonstrate the use of the PET. Tasks related to record, consent and privacy policy are removed for this analysis as the **Simple Disclosure analysis** analyses the security provided by the applied technology - in this case, PKI, while these tasks do not change the protected data object. When Simple Disclosure analysis is done, a table is returned which shows the data objects and their visibility for different counterparts (see Fig. 15). We can see, that the PLT owns key pair A (marked as O in the table) and the user device owns the key pair B. In addition, the data, after being encrypted, is hidden from the controller, which means that they cannot see the contents as a plain text when transferring the data between the subject and processor (marked as H in the table). We can also see, which data is visible for which role (marked as V). Since the encrypted data is decrypted after

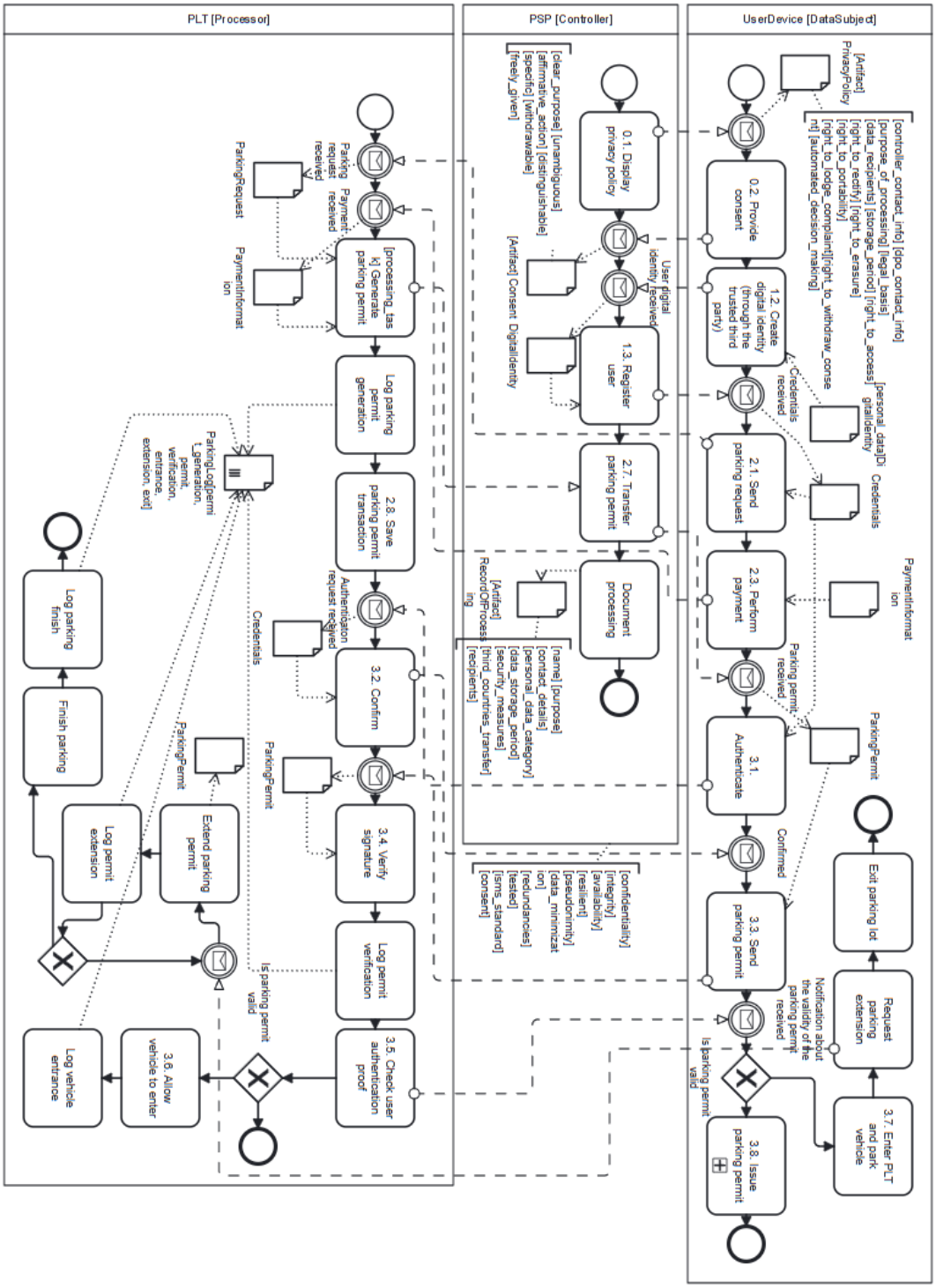


Figure 12. Log Processing Tasks Sub-process Model

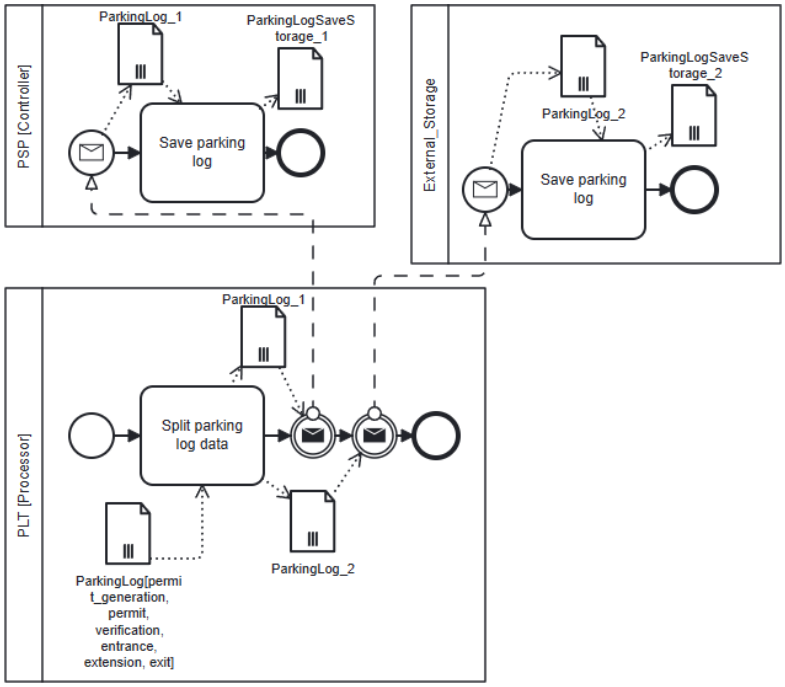


Figure 13. Logs Storing Sub-Process

receiving it, it is also visible to the decrypting party. Lastly, the table shows that the data objects - ParkingRequest and ParkingPermit - move through a secure channel (marked as S). The protected data objects (ParkingRequest and ParkingPermit) are visible only to the party who generates it (User and PLT) and to the party that should have access to the data original form (PLT and User). In contrast, the intermediate party (PSP) does not have access to the data and only transfers the protected data objects. This confirms, that the PKI technology can provide secure data transfer between different system counterparts, and the data contents are visible to only necessary parties. The Manage Payment and Register User Pleak models can be found in Appendix VI and the analysis results for all the remaining models are found in Appendix VII.

### 4.2.2 Analyse Statistical Data Sub-Process Enhanced with MPC

The sub-process **Store Logs** from the Analyse Statistical Data is analysed with the Pleak tool. This part contains the MPC technology usage, and we can analyse how the data can be accessed by different system counterparts. We re-design the sub-process model using the PE-BPMN editor to label the Secure Secret Sharing task and the channels (see Fig. 16). Then, the **Simple Disclosure analysis** is run on the storing sub-process.

As a result (see Fig. 17), the table with the same concept as described in the Request Parking Pleak analysis chapter is generated. From this overview, we can see that the

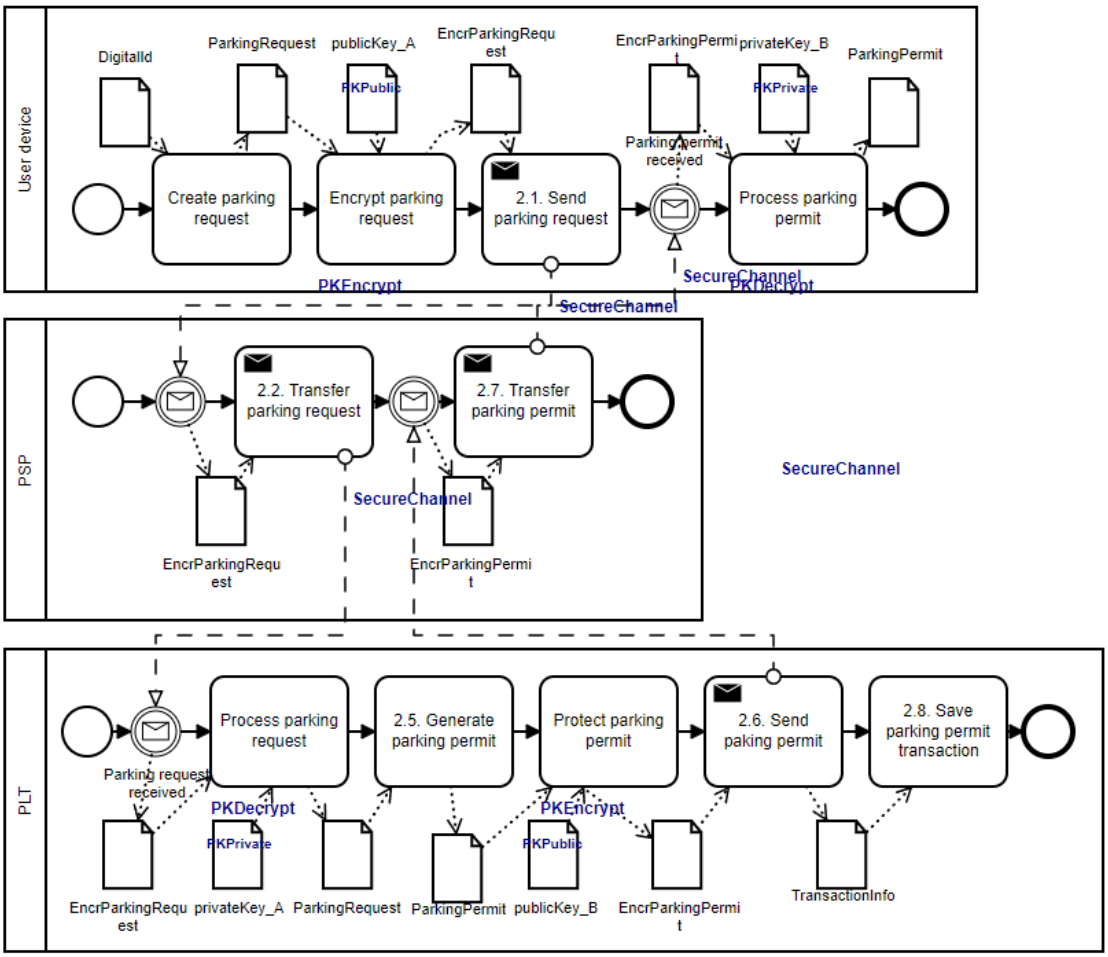


Figure 14. Request Parking Sub-Process as a PE-BPMN Model

| # | DigitalId | EncrParkingPermit, ParkingPermit | EncrParkingRequest, ParkingRequest | TransactionInfo | privateKey_A | privateKey_B | publicKey_A | publicKey_B |
|---|---|---|---|---|---|---|---|---|
| **PLT** | - | V | V | V | O | - | - | O |
| **PSP** | - | H | H | - | - | - | - | - |
| **User device[DataSubject]** | O | V | V | - | - | O | O | - |
| Shared over | - | S | S | - | - | - | - | - |

Figure 15. Request Parking Leakage Analysis

PLT owns the split-up ParkingLog objects. These are transferred for storage through a secure channel to the PSP and the trusted external storage. We can see, that the storage information of these logs is visible to the PSP and the external storage, but the actual contents of the logs are hidden from them. The data is securely split before transferring, which causes the data to be hidden from the storing parties, and they only have the storage information about these logs.

## 4.3 Summary

In this chapter, we re-designed the process models to depict the use of PETs, from which we selected the PKI and MPC technologies. The Analyse Statistical Data uses MPC to secure the data processing, whereas the Register User, Request Parking, and Manage Payment processes use PKI technology. We created the PE-BPMN models and used the Pleak tool to analyse these designs and answer the **SRQ3** - *"How does the Pleak tool help select the privacy-enhancing technology?"*. The Pleak tool helps to analyse the effectiveness of the selected PETs by giving an overview of the data objects used in the process and their visibility between different counterparts of the process. We can assess, whether the selected technology preserves the privacy of vulnerable data. In addition, we get an overview of the visibility of each data object for the different parties in the scenario.

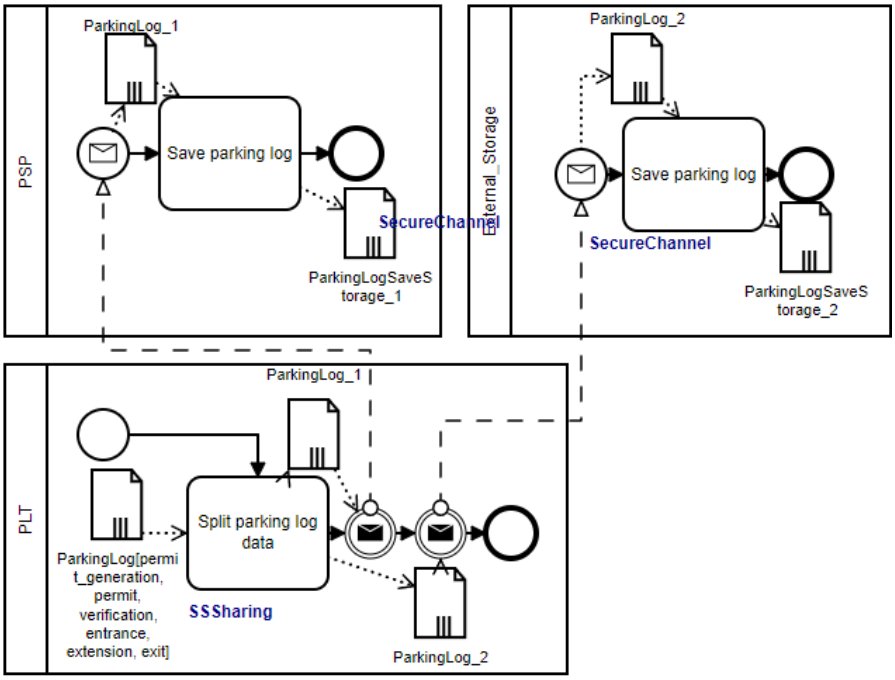


Figure 16. Logs Storing Sub-Process as a PE-BPMN Model

| # | ParkingLogSaveStorage_1 | ParkingLogSaveStorage_2 | ParkingLog[permit_generation, permit, verification, entrance, extension, exit], ParkingLog_1, ParkingLog_2 |
|---|---|---|---|
| **External_Storage** | - | V | H |
| **PLT** | - | - | O |
| **PSP** | V | - | H |
| Shared over | - | - | S |

Figure 17. Log Process Analysis Result

# 5 Conclusion

In this thesis, we used the tool-supported privacy analysis method introduced in [3] to analyse the Smart Parking scenario presented in [2]. To answer **MRQ** - *How can the DPO and Pleak tools help analyse the parking process compliance with the GDPR?* - we split it into the following sub-questions. To answer **SRQ1**, we defined the requirements that organisations have to follow for privacy-preserving data processing. We described the DPO Tool and Pleak tool and their use cases in the analysis. The DPO Tool analyses compliance with the GDPR, whereas the Pleak tool analyses data leakage in the process. In addition, we analysed the scenario and identified the sensitive data. For **SRQ2**, the sub-processes of the parking scenario were analysed using the DPO Tool, which identified multiple issues such as missing privacy policy, missing attributes from the system regarding security and privacy, and missing records of processing. The processes were re-designed and re-analysed to verify the changes to the processes. Lastly, to answer **SRQ3**, the models were enhanced with PKI and MPC technologies, verified with the DPO Tool once again, and then analysed with the Pleak tool using Simple Disclosure analysis to identify data leakages.

## 5.1 Answers to Research Questions

**SRQ1: What requirements do organisations need to meet regarding business processes?** We reviewed the privacy principles that systems must follow to process data in a privacy-preserving manner. The principles are Privacy by design, data minimization, purpose and storage limitation, anonymisation and pseudonymisation, transparency, and secure processing (CIA triad). We reviewed the GDPR and described the articles, which gave us a set of requirements that can be analysed with the DPO Tool. The smart parking business processes were analysed and the non-compliance issues were discovered. We identified the sensitive data in the smart parking scenario which includes the **digital identity** of the user and **payment information**. Digital identity contains information about the user that can be used to identify the person. The payment information also includes information about the user that can be used to link to them.

**SRQ2: How does the DPO tool provide support in privacy analysis?** We analysed the smart parking sub-processes to identify the GDPR compliance issues. The analysis was supported by the DPO Tool, to which we provided as the input the As-Is BPMN models and the DPO Tool provided the feedback containing compliance issues. Additional input with the key GDPR concepts like choosing the data subject, controller, processor and labelling the personal data object and the processing task were provided. The feedback contains found issues in the process model and the corresponding article numbers from the GDPR, which enables checking the regulations and the contents of the violated articles. The models were re-designed according to the feedback given by the DPO Tool to fix the compliance issues and then the tool was used to validate the changes.

**SRQ3: How does the Pleak tool provide support in privacy analysis?**We complemented the GDPR-compliant BPMN models with the PKI and MPC technologies and validated the correctness of the structure and syntax using the DPO Tool. The PE-BPMN models were then re-designed using the PE-BPMN and Leaks-When editor in the Pleak tool to depict the use of the selected PET in the process. The privacy-enhanced models were then analysed using the Simple Disclosure analysis, which gave an overview of the data objects and their visibility in the different parts of the process. The analysis can be used for detecting data leakages in the process.

## 5.2 Lessons Learnt

During the process redesign with privacy-preserving measures, there were different learning points at the preliminary stage and during the analysis:

1. **Define the privacy requirements before analysis is started** - Before the analysis, defining the requirements the processes need to meet is an important part of starting the procedure. To understand, which privacy issues the sub-processes might have, the regulations [4] should be used to define the requirements and then analyse the processes according to these requirements. This gives an idea of which parts of the business process are lacking privacy-preserving measures. Furthermore, understanding what the business process is missing helps to acknowledge the tools' functionalities and feedback.

2. **Learn to use the tools for privacy analysis** - Another preliminary requirement is the correct usage and how to interpret the feedback to make correct model changes. Understanding the feedback given by the tools assists us in being aware of the missing privacy-preserving measures. It is possible to see which requirements are not met by the processes and whether the privacy-preserving measures are implemented incorrectly. Furthermore, the Pleak tool helps to analyse the correct application of the selected PETs and their effectiveness in secure data processing. In addition, understanding the visibility matrix helps us to understand, which counterparts can see which data objects. This matrix provides an overview of possible data leakages in the system.

3. **Separate personal data objects for analysis** - During the analysis, the understanding that a singular personal data object should be analysed at once, was missing. This led to a situation, where the permit issuing process compliance could not be evaluated correctly since we should evaluate the processes for each of the personal data objects separately. Thus, the process had to be split into two different sub-processes which each on their own consumed one personal data object. It is important to identify the personal data objects during the early stage of the process analysis which allows us to recognise the business processes that might be using

multiple objects. Furthermore, this allows the early distinction of the processes and correct analysis of the processes.

4. **Select suitable PETs** - Before starting to re-design the business processes, identifying the possible applicable PETs can help better plan the application of privacy-preserving measures. The realization of the need for a statistical analysis model after trying to apply the MPC technology on the parking sub-processes took some time and the possibilities to demonstrate the application of the mentioned PET had to be rethought. As a result, the knowledge that the MPC does not apply correctly to the existing sub-processes came after the models had been constructed. This resulted in the design of a new process model to which the MPC could be applied.

5. **Follow the syntax** - Since both of the tool's inputs depend on BPMN models, the syntax must be followed. The DPO Tool gave instant feedback on syntax errors occurring in the models given as input, making it easy to find the mistakes in the model and fix them.

## 5.3 Implications for the Smart Parking Scenario

As a result of the smart parking business process privacy analysis, models for Register User, Request Parking, Manage Payment and Analyse Statistical Data sub-processes were designed. These models depict the flows of the sensitive data objects. The measures required by the regulations have been applied to the business processes. Before sending any data for processing, the user is provided with a privacy policy and the knowledge of how their data is processed. After the policy is provided, the user is required to consent to process their data. In addition, the processor follows the requirements of secure data processing, including following the CIA triad, data minimization principle, application of PETs, etc. Regarding the processor, the task, which works with the personal data object, is clearly distinguished from the tasks. The task is also recorded, and the record is generated, which includes the information about the data processing.

Lastly, the registering sub-process, along with the payment and permit generation process, applies the PKI technology, resulting in the encrypted personal data being transported between different parties. The data is decrypted and only visible for processing. The application of MPC did not turn out to be possible for the provided sub-processes. Nonetheless, a statistical analysis was conducted on the whole parking scenario. This allowed us to demonstrate the possibility of splitting the processing logs, securing them and storing the splits in different storage. This results in a situation where the information is secured and the storing parties only have the information about the storage.

## 5.4 Limitations

The analysis is done on BPMN models based on a general smart parking scenario, which means that the produced models should not be taken as complete for usage in the real-life smart parking systems. The PE-BPMN models give a basis for improving the security of smart parking systems and following a privacy-preserving methodology for processing personal data. This approach can help secure the User-Parking Lot interaction but further development should be considered to evaluate the effectiveness of the provided PETs on organisation-specific business processes. In addition, the following company-specific requirements are not taken into account in this analysis:

- **Payment system of the Parking Service or/and users bank** - This introduces an external component not under the parking system control. These organisations have to follow the regulations (the GDPR if located in the EU) and have their internal data processing requirements.
- **Free parking times** - When is it actually required to use the system to register your parking and when is it necessary to proceed with payment - this can provide an extra set of requirements to process these scenarios.
- **Authentication into the application** - This introduces a number of third parties to the system and each has to follow the GDPR when located in the EU and have their internal requirements as well.
- **Access control within the Service Provider** - This is company-specific and determines, who has which rights within the system. This also includes the access of different roles to the data that is being processed.

The thesis recommends privacy-preserving measures for the parking business processes to make the processes GDPR compliant. This means that for the smart parking business processes, the DPO tool is irrelevant outside the EU, setting boundaries for analysing similar processes and making recommendations outside the EU. Furthermore, the PETs chosen for enhancing the parking processes - public key infrastructure and multi-party computation - are selected because of their wide usage in different systems. Alternative technologies should also be considered for other systems as the PETs provided in this thesis are not a universal choice for all the systems.

## 5.5 Future Work

In future work, the following developments of this work are possible. First, **application of the method in running service providers' processes** is one possible development for this thesis. As the thesis focuses on certain business processes extracted from the smart parking scenario, more validation is needed to generalise the results. The processes could

be organisation-specific to give a better overview of the possibilities of applying PETs to smart parking business processes. This means that one possible development path would be to choose some organisation-specific business process related to smart parking to validate the method even more in the smart parking scenario. Secondly, **application of the method to a scenario from another domain** is another path for development in order to validate the method for other types of services. This thesis and previous work focused on transportation-related services, but the method could be used to analyse retail services, banking systems, etc. This would also help generalise the use of the provided method to analyse different business processes and apply the method to a wider range of businesses. Finally, to be able to compare the method, **application of other tools and/or methods** could be done. This would cover the smart parking scenario with a wider range of tools and different methods which would enable the comparison of the different results for this scenario.

# References


[1] A. Kalašová, K. Čulík, M. Poliak, and Z. Otahálová, "Smart parking applications and its efficiency," *Sustainability*, vol. 13, no. 11, 2021.

[2] P. Dzurenda, F. Jacques, M. Knockaert, M. Laurent, L. Malina, R. Matulevičius, Q. Tang, and A. Tasidou, "Privacy-preserving solution for vehicle parking services complying with EU legislation," *PeerJ*, vol. 8, p. e1165, 12 2022.

[3] M. Bakhtina, R. Matulevičius, and M. Seeba, "Tool-supported method for privacy analysis of a business process model," *Journal of Information Security and Applications*, vol. 76, p. 103525, 2023.

[4] "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 on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016. Last accessed on 30.01.2024.

[5] R. Abraham, J. Schneider, and J. vom Brocke, "Data governance: A conceptual framework, structured review, and research agenda," *International Journal of Information Management*, vol. 49, pp. 424–438, 2019.

[6] M. Knockaert, M. Laurent, L. Malina, R. Matulevicius, M. Petrocchi, M. Seeba, Q. Tang, A. Tasidou, and J. Tom, *Privacy-by-Design in Intelligent Infrastructures*, pp. 309–343. No. 51 in Collection du CRIDS, Larcier, 2021.

[7] A. J. Biega, P. Potash, H. Daumé, F. Diaz, and M. Finck, "Operationalizing the legal principle of data minimization for personalization," in *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR '20, (New York, NY, USA), p. 399–408, Association for Computing Machinery, 2020.

[8] J. Buchmann, E. Karatsiolis, and A. Wiesmaier, *Introduction to public key infrastructures*, vol. 36. Springer, 2013.

[9] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, and Y. an Tan, "Secure multi-party computation: Theory, practice and applications," *Information Sciences*, vol. 476, pp. 357–372, 2019.

[10] M. Von Rosing, S. White, F. Cummins, and H. De Man, "Business process model and notation-bpmn.," 2015.

[11] R. Matulevičius, J. Tom, K. Kala, and E. Sing, "A method for managing gdpr compliance in business processes," in *Advanced Information Systems Engineering*

(N. Herbaut and M. La Rosa, eds.), (Cham), pp. 100–112, Springer International Publishing, 2020.

[12] E. Sing, "A meta-model driven method for establishing business process compliance to GDPR," Master's thesis, University of Tartu, 2018.

[13] P. Pullonen, J. Tom, R. Matulevičius, and A. Toots, "Privacy-enhanced BPMN: enabling data privacy analysis in business processes models," *Software and Systems Modeling*, vol. 18, pp. 3235–3264, 2019.

# Appendix

# I. Glossary

| | |
|---|---|
| AV | Autonomous Vehicle |
| BPMN | Business Process Model Notation |
| CIA | Confidentiality, Integrity, Availability |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| ISMS | Information Security Management System |
| MPC | Multi-Party Computation |
| MRQ | Main Research Question |
| PE-BPMN | Privacy-Enhanced Business Process Model |
| PET | Privacy-Enhancing Technology |
| PKI | Public Key Infrastructure |
| PLT | Parking Lot Terminal |
| PSP | Parking Service Provider |
| RQ | Research Question |
| SRQ | Sub-Research Question |

# II. Models depicting the scenario

Figure 18 describes the Register User sub-process without the use of data objects. The process has two counter parts, the user device and the PSP.

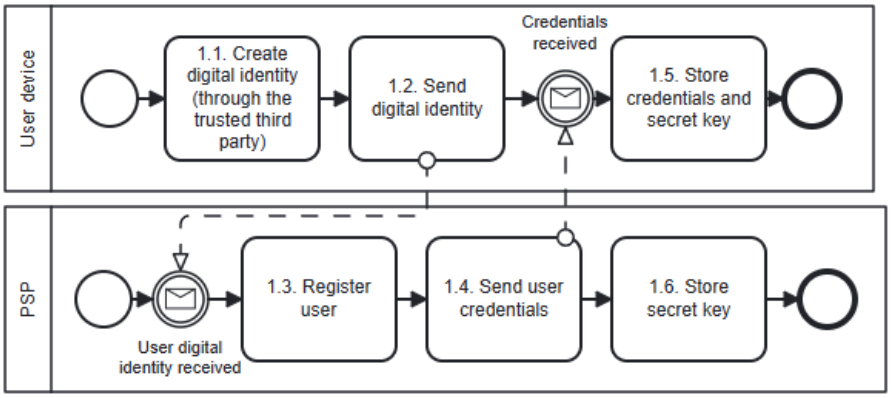


Figure 18. Register User sub-process

Figure 19 depicts the Park Vehicle subprocess, where there are two counterparts: User Device and PLT. In case of invalid parking permit, the system goes to the Issue Parking Permit sub-process to generate a new permit.

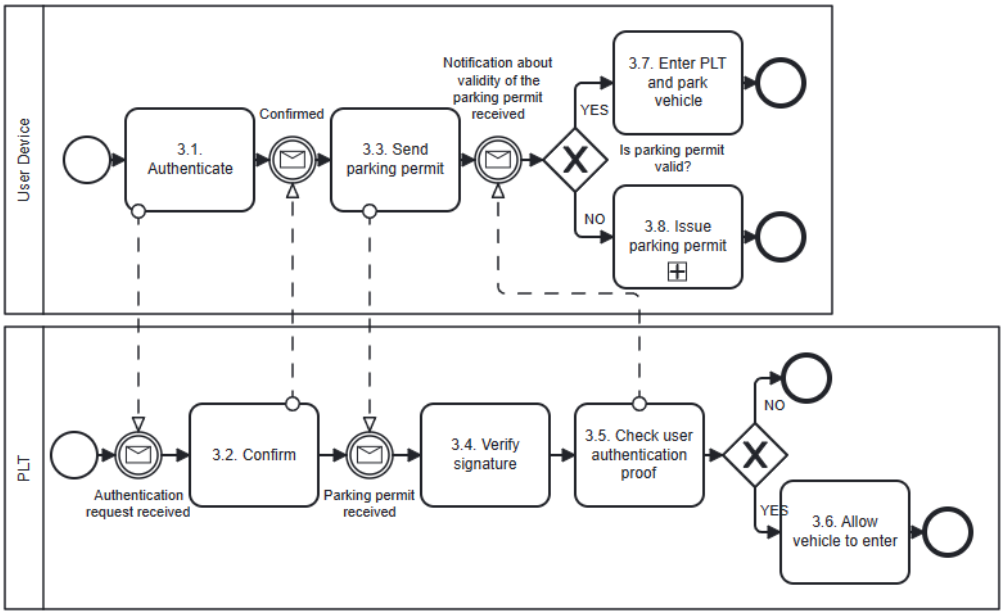


Figure 19. Park Vehicle sub-process

In Figure 20, the Parking Time Extension sub-process is described. The extension is possible, if the permit is available, otherwise the system issues a new parking permit.

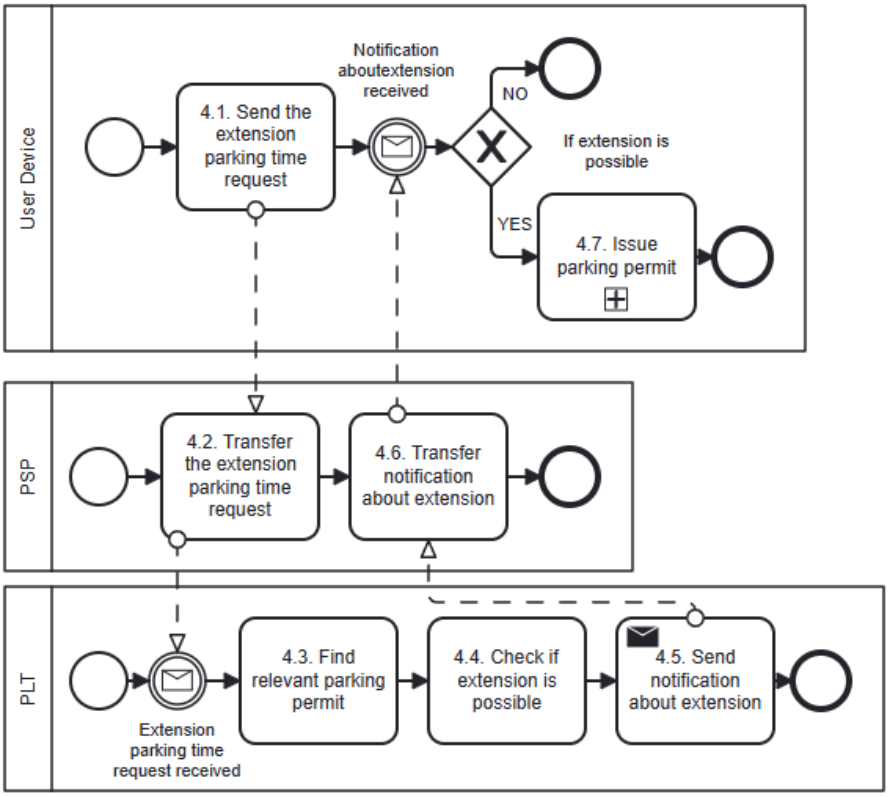


Figure 20. Parking Time Extension sub-process

# III. Privacyless models

Figure 21 describes the Register User sub-process with the use of the data objects. The personal data object, that needs protection, is **DigitalIdentity**.

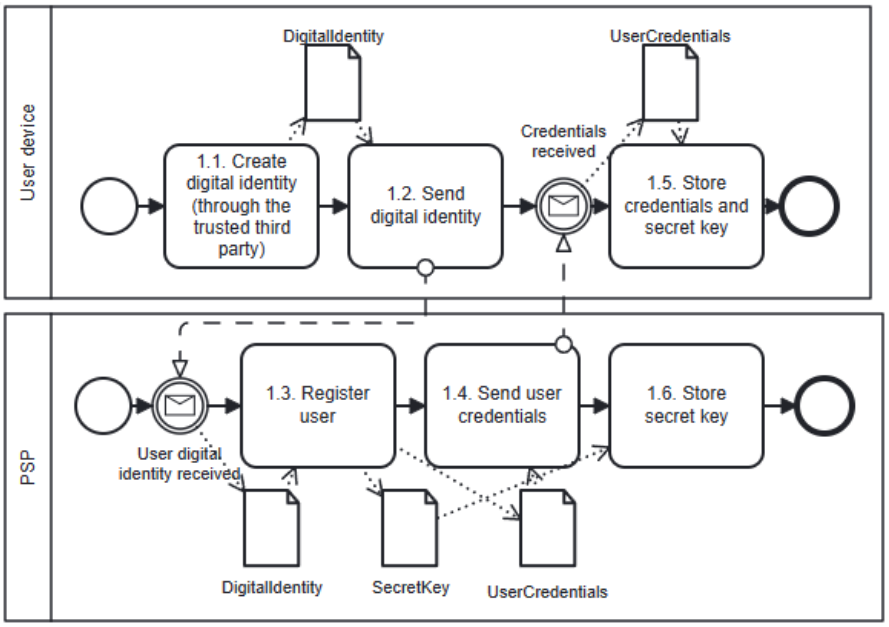


Figure 21. Register User sub-process with data objects

Figure 22 describes the Manage Payment sub-process with the use of the data objects. The personal data object, that needs protection, is **PaymentInformation**.

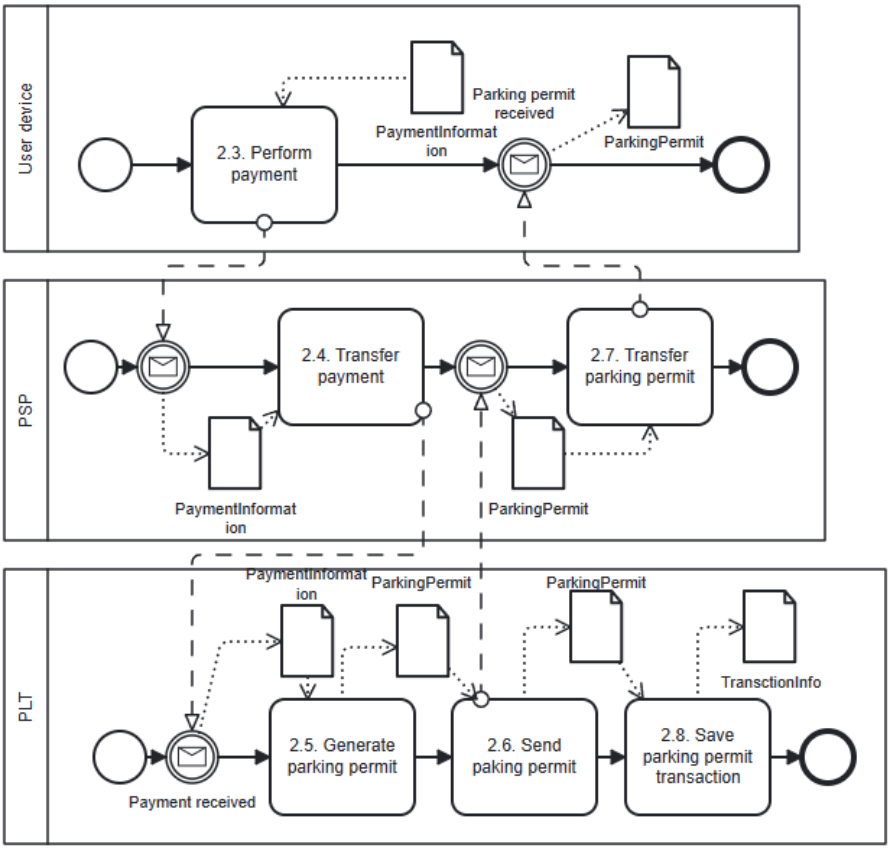


Figure 22. Manage Payment sub-process with data objects

Table 2 depicts the exact inputs used in the DPO Tool for each sub-process in order to conduct GDPR compliance analysis.

Table 2. DPO Tool Inputs for the Sub-Processes

| **Sub-Process** | **Data subject** | **Controller** | **Processor** | **Processing task** | **Personal Data object** |
|---|---|---|---|---|---|
| Register User | User Device | PSP | PSP | Process Digital Identity | DigitalIdentity |
| Manage Payment | User Device | PSP | PLT | Process Payment | Payment Information |

# IV. GDPR Compliant models without PETs

Figure 23 describes the GDPR-compliant Manage Payment sub-process. The reconstructed diagram follows the steps provided in Chapter 3.

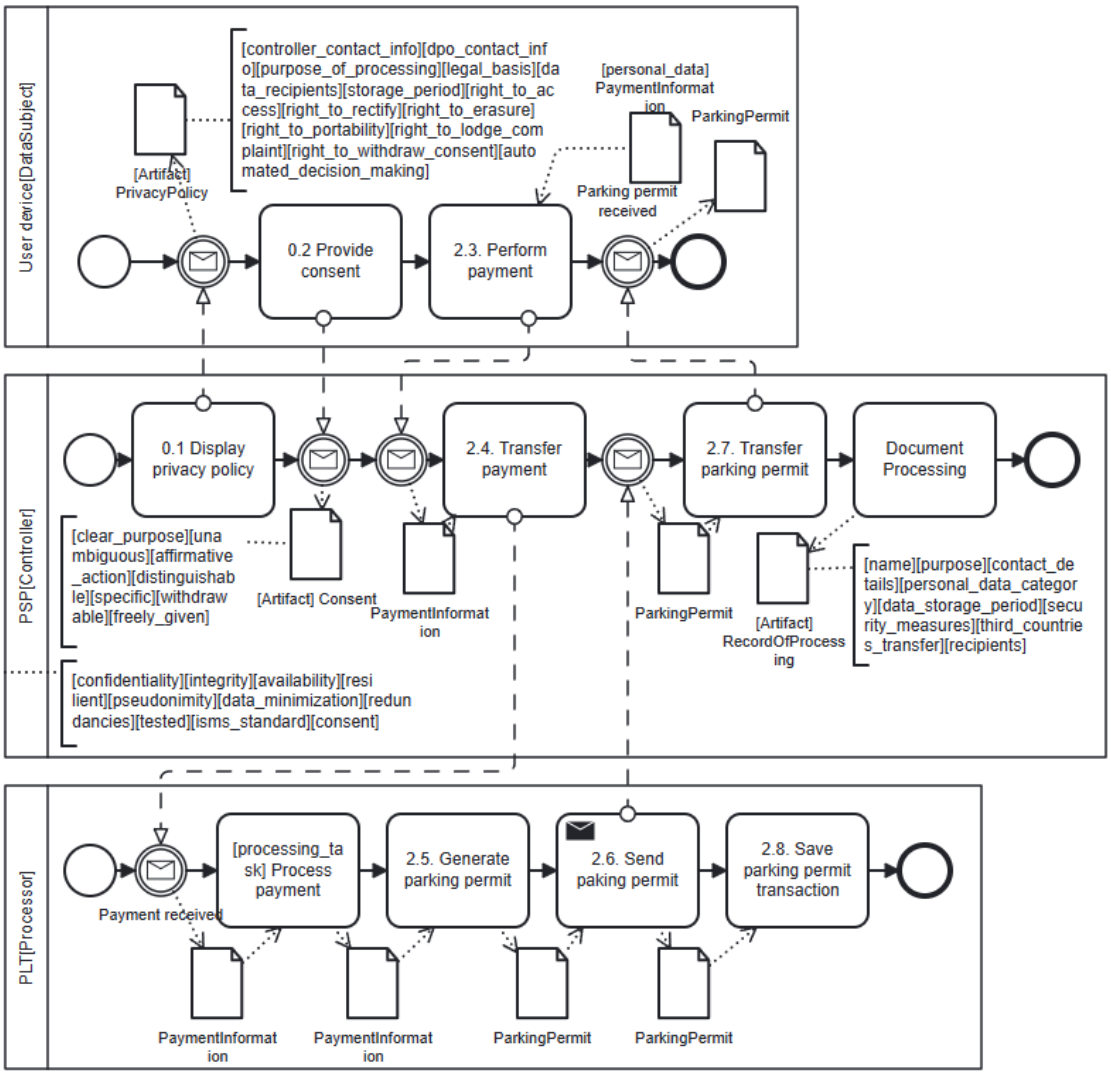


Figure 23. Manage Payment GDPR compliant

Figure 24 describes the GDPR-compliant Register User sub-process. The reconstructed diagram follows the steps provided in Chapter 3.

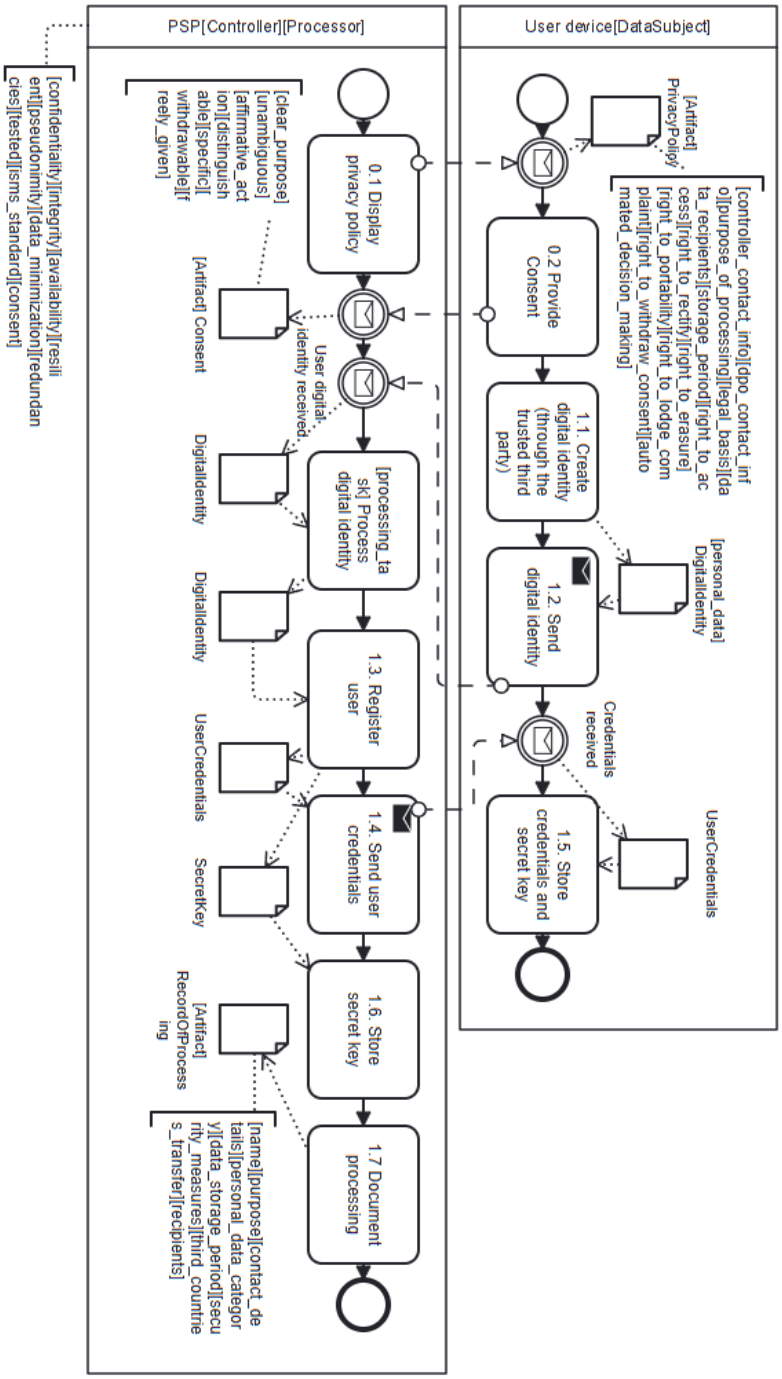


Figure 24. Register User GDPR compliant

# V. GDPR Compliant models using PKI

Figure 25 describes the GDPR-compliant Manage Payment sub-process which uses the PKI technology.

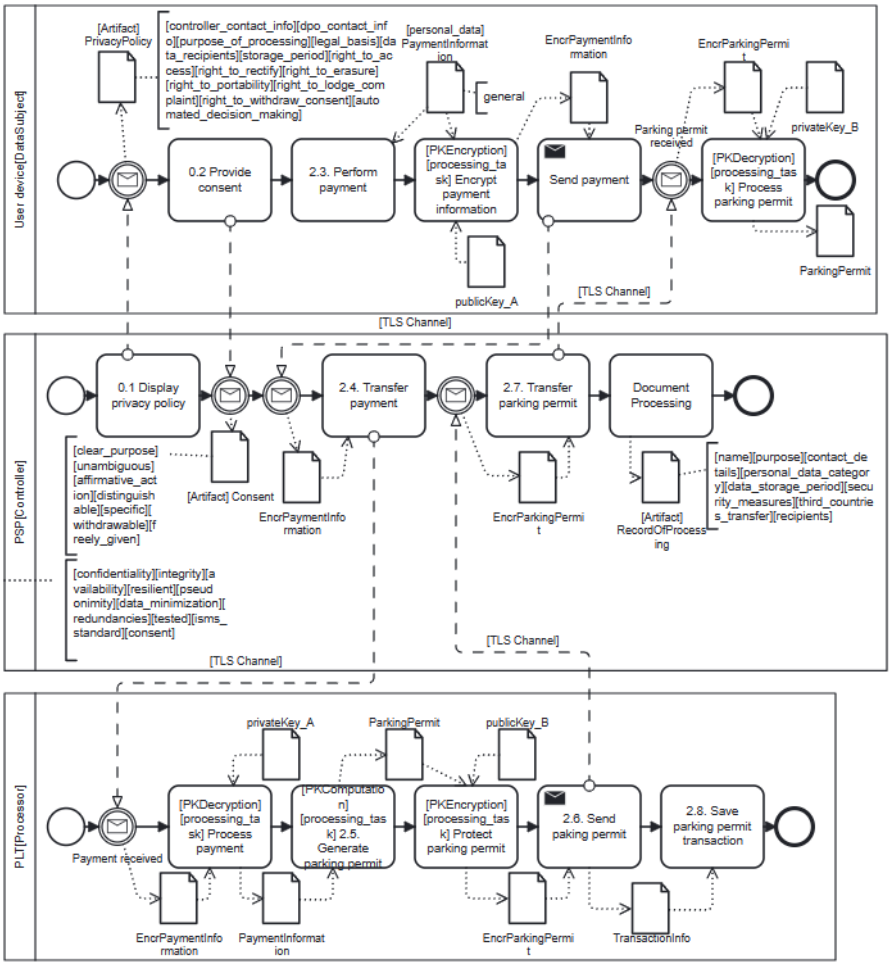


Figure 25. Manage Payment PKI

Figure 26 describes the GDPR-compliant Register User sub-process which uses the PKI technology.

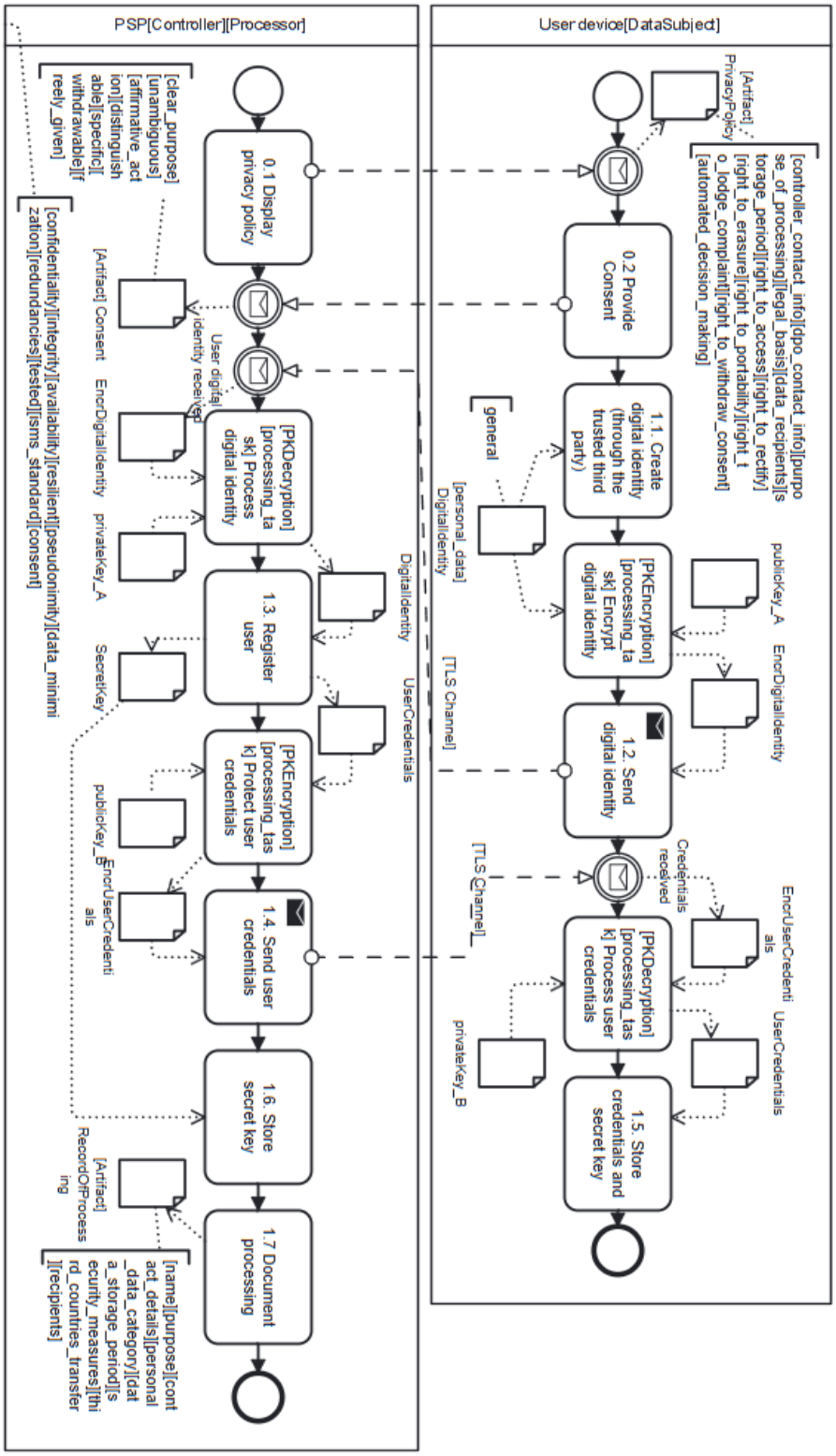


Figure 26. Register User PKI

# VI. Models for Pleak analysis

Figure 27 demonstrates the re-designed Manage Payment model which is used for the Pleak tool analysis input. It depicts the use of PKI technology.

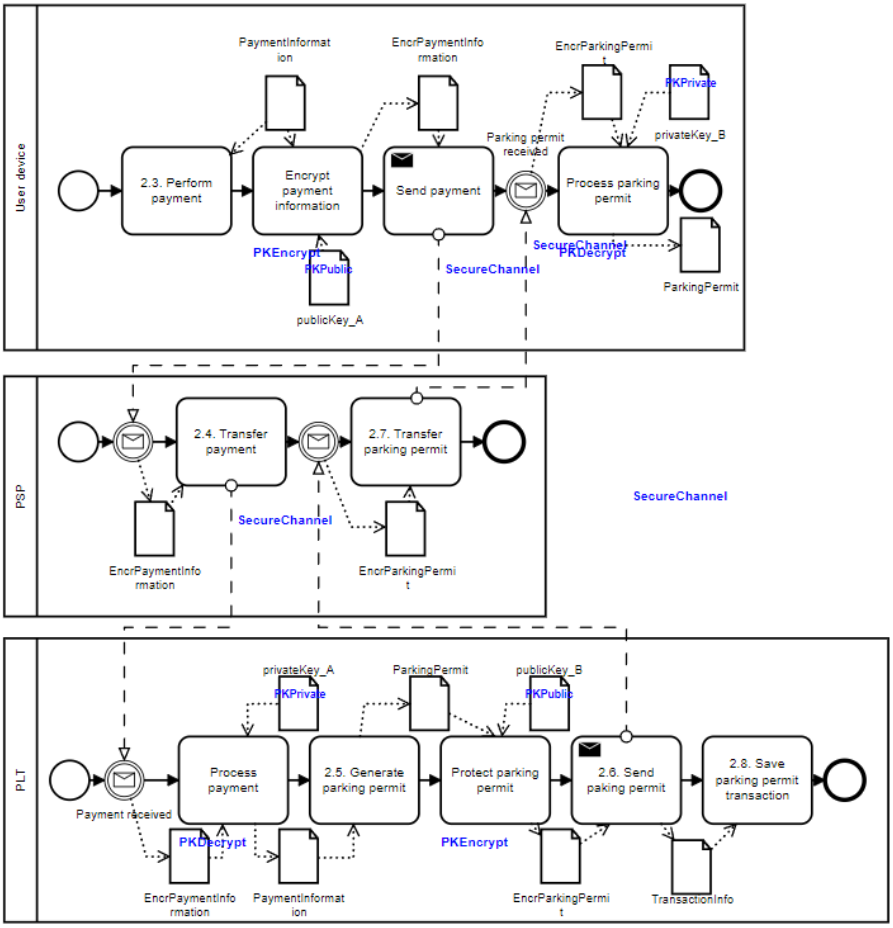


Figure 27. Manage Payment Pleak model

Figure 28 demonstrates the re-designed Register User model which is used for the Pleak tool analysis input.

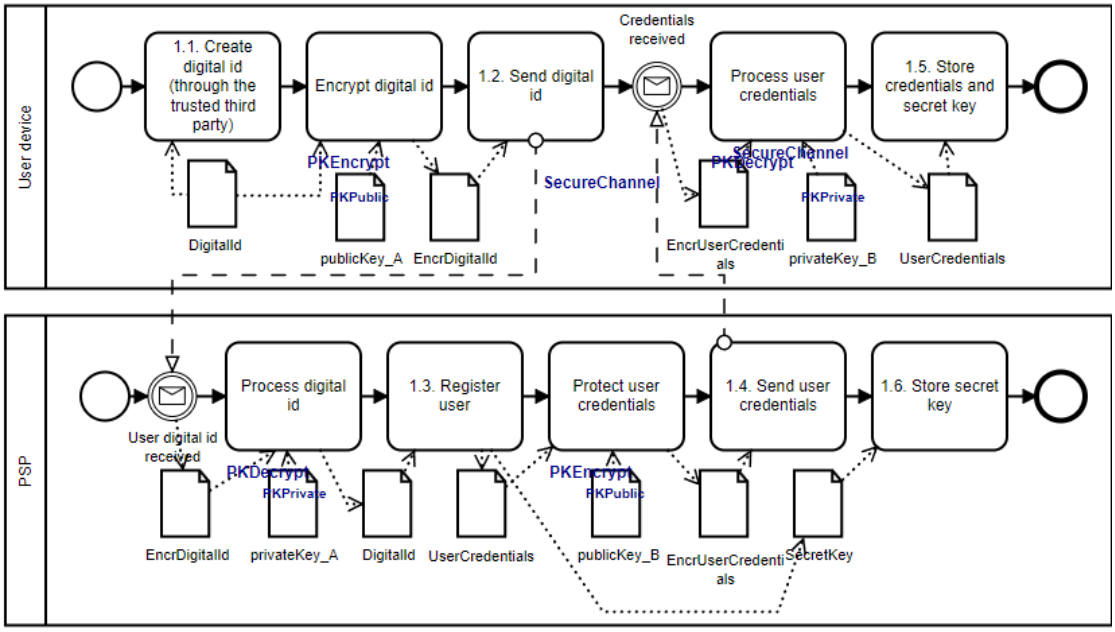


Figure 28. Register User Pleak model

# VII. Pleak analysis results

Figures 29 and 30 contain the results for the Manage Payment and Register User pleak analysis. It covers the visibility and ownership of the different data objects in the corresponding processes.

| # | EncrParkingPermit, ParkingPermit | EncrPaymentInformation, PaymentInformation | TransactionInfo | privateKey_A | privateKey_B | publicKey_A | publicKey_B |
|---|---|---|---|---|---|---|---|
| **PLT** | V | V | V | O | - | - | O |
| **PSP** | H | H | - | - | - | - | - |
| **User device** | V | O | - | - | O | O | - |
| Shared over | S | S | - | - | - | - | - |

Figure 29. Manage Payment leakage analysis

| # | DigitalId, EncrDigitalId | SecretKey | EncrUserCredentials, UserCredentials | privateKey_A | privateKey_B | publicKey_A | publicKey_B |
|---|---|---|---|---|---|---|---|
| **PSP** | V | V | V | O | - | - | O |
| **User device** | O | - | V | - | O | O | - |
| Shared over | S | - | S | - | - | - | - |

Figure 30. Register User leakage analysis

# VIII. Licence

## Non-exclusive licence to reproduce thesis and make thesis public

I, **Sander Truu**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   **Tool-Supported Privacy Analysis of Smart Parking**,

   supervised by Mariia Bakhtina and Raimundas Matulevičius.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Sander Truu
***15/05/2024***