Department of Computer Science

Towards a Principled Approach for Engineering Privacy by Design

Majed Alshammari and Andrew Simpson

CS-RR-16-05

Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD

Towards a Principled Approach for Engineering Privacy by Design

Majed Alshammari and Andrew Simpson

Department of Computer Science
University of Oxford

June 6, 2016

Abstract

Privacy by Design has emerged as a proactive, integrative, and creative approach for embedding privacy requirements into the early stages of the design of information and communication technologies, business practices, and physical designs and infrastructures. Yet, Privacy by Design is no 'silver bullet'. Challenges involved in engineering Privacy by Design include a lack of holistic, systematic and integrative methodologies that address the complexity and variability of privacy, and support the translation of its foundational principles into engineering activities. In some ways this is understandable: the approach was developed to take into account a range of sources and standards. However, a consequence is that its foundational principles are given at a high level of abstraction without accompanying methodologies and guidelines to elicit concrete privacy requirements and specify appropriate design decisions. In this report, we analyse three privacy requirements engineering methods from which we derived a set of criteria that meet these challenges. In essence, these criteria are in consonance with the foundational principles of Privacy by Design to aid software engineers in identifying activities that can lead to privacy harms in a concrete and meaningful manner, and specifying appropriate design decisions at an architectural level in a rational and positive-sum manner. To this end, we put forward a proposal for engineering Privacy by Design that can be developed upon these criteria.

1 Introduction

Privacy, as a human right, is defined as a multi-faceted concept, which has several aspects with a variety of meanings in various contexts. In addition, privacy is subjective in its nature, as it is derived from society demands, expectations and culture, which are influenced by several factors, such as political, social and economic changes as well as information technology advancements [WB90, OGD+05]. This, in turn, introduces complexity and variability [DFF14]. To address this complexity and variability in the context of information

and communication technologies, laws and regulations alone are not sufficient in protecting individuals' privacy [HZNF15, Spi12]. In particular, laws and regulations need to be accompanied with holistic methodologies and guidelines to aid software engineers, architects, designers and developers to address this complexity and variability in the software development process.

As a response, Privacy by Design has been advocated by the former Information and Privacy Commissioner of Ontario, amongst others, and is intended to be a proactive, integrative and creative approach for embedding privacy requirements into the early stages of the design process to achieve an adequate level of privacy protection and meet regulatory compliance [Cav09]. The foundational principles of Privacy by Design are based on the Fair Information Practice Principles (FIPPs) [Cav10], and act as a universal framework for incorporating privacy into three main areas of application: information and communication technologies, business practices, and physical designs and infrastructures [CSC14]. In 2010, Privacy by Design was recommended as an international privacy standard by the participants of the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem [CSD+10, Cav12]. Since then, Privacy by Design has been recommended by legislation in various jurisdictions, such as the proposal of the EU Data Protective Directive[1], and the U.S. Federal Trade Commission (FTC)[2]. This implies that Privacy by Design is likely to become a legal requirement in several jurisdictions.

Yet, Privacy by Design is no 'silver bullet'. Challenges involved in engineering Privacy by Design include a lack of holistic, systematic and integrative methodologies that address the complexity and variability of privacy, and support the translation of its foundational principles into engineering activities. In some ways this is understandable, as this approach was developed to take into account a range of sources and standards. However, a consequence is that its foundational principles are given at a high level of abstraction without accompanying methodologies guidelines to elicit concrete privacy requirements and specify appropriate design decisions. This, in turn, introduces significant challenges by relying on software engineers' expertise in respect of understanding and translating privacy regulations and principles into concrete privacy requirements. This approach, however, serves as a reference framework in its current state and does not address the establishment of engineering methodologies. Accordingly, Privacy Engineering has emerged as a new discipline that aims to apply engineering principles and processes in developing, deploying and maintaining systems in a systematic and repeatable way, to achieve an acceptable level of privacy protection [DFF14]. To distinguish between these concepts, Privacy by Design (PbD) aims to explain "What to do" to achieve an appropriate level of privacy protection, whereas Privacy Engineering (PE) aims to explain "How to do it" by defining privacy as a quality attribute in systems engineering [CSC14]. In other words, it focuses on developing and evaluating

[1]European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Retrieved from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [Accessed 1 February, 2016]

[2]Federal Trade Commission: Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission. Retrieved from: https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf [Accessed 1 February, 2016]

methods, techniques and tools that identify and address privacy concerns in a systematic manner during the development process of socio-technical systems [GdA16]. In this context, we will consider the adoption of Privacy by Design into software engineering with a focus on information and communication technologies (ICTs) as an area of application of Privacy by Design.

In this report, we analyse three privacy requirements engineering methods to understand how those methods address the main challenges, from which we derive a set of criteria that meet these challenges and support the process of engineering Privacy by Design. In essence, these criteria are in consonance with the foundational principles of Privacy by Design to aid software engineers in identifying system activities that cause privacy harms in a concrete and meaningful manner, and specifying appropriate design decisions at an architectural level in a rational and positive-sum manner. To this end, we put forward a proposal for engineering Privacy by Design that can be developed upon these criteria.

The rest of this report is organised as follows. Section 2 explores the main challenges of engineering Privacy by Design and illustrates how three privacy requirements engineering methods address those challenges. In addition, it explains a set of derived criteria that meet these challenges and support the process of engineering Privacy by Design. Section 3 gives a relatively detailed discussion of the Privacy by Design approach and explains its shortcomings in respect of these criteria. Section 4 describes the proposed approach for engineering Privacy by Design as a means of addressing the gaps by eliciting concrete privacy requirements and specifying an appropriate design that fulfils these requirements. Section 5 introduces the ePetition system, which implements the European Citizens' Initiative, as a case study. Section 6, illustrates the main elements of the proposed approach through the case study. Finally, in Section 7, we summarise the contribution of this report and outline our plans for future work in this area.

2 Privacy harms identification as a fundamental step

The identification and analysis of potentially harmful activities play a crucial role in engineering Privacy by Design. In more detail, an appropriate privacy threat analysis framework is considered to be a cornerstone of identifying system activities that cause privacy harms, conducting privacy impact analysis and assessment, eliciting privacy requirements, and specifying appropriate architectural designs to achieve an acceptable level of privacy protection [DWS+11].

In this section, we will explain the main challenges of engineering Privacy by Design. Then, we will analyse three existing privacy requirements techniques and derive a set of criteria that aid software engineers in eliciting concrete privacy requirements and specifying appropriate designs that fulfil these requirements at an architectural level. We start, in Section 2.1, by explaining the main challenges and the motivation behind establishing these criteria.

2.1 The challenges of engineering Privacy by Design

Engineering Privacy by Design involves significant challenges, which include a lack of methodologies that can be adopted to integrate the foundational principles of Privacy by Design into the engineering process. Such methodologies are expected to aid software engineers in analysing functional requirements, eliciting privacy requirements and making appropriate design decisions that fulfil these requirements [GTD11].

With respect to the analysis and design stages of the engineering process, these challenges can be decomposed into a number of concrete challenges, as summarised by Gürses et al. [GTD11].

The first challenge concerns addressing the complexity of privacy as a legal, social and political concept. This complexity challenges software engineers to understand and translate various perceptions and concerns into operational requirements [GTD11]. Therefore, an appropriate interpretation of abstract definitions, principles and guidelines, such as the foundational principles of Privacy by Design, requires a specific kind of expertise [GTD11]. Furthermore, existing privacy guidelines are usually stage or domain specific [NCM+15]. Indeed, a privacy threat analysis requires specifying privacy protection goals and objectives, which are driven from relevant privacy legislation, principles and guidelines [Spi12]. For the purpose of developing a generic and holistic methodology, we emphasise the importance of adopting universal privacy principles and standards to be served as generic principles and guidelines. For example, the Organisation for Economic Co-operation and Development (OECD) published Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Org13]. These guidelines have much in common with Fair Information Practice Principles (FIPPs) [Uni73], and have served as a foundation for privacy and data protection laws and regulations in many jurisdictions [SC09]. This means that these guidelines are a set of comprehensive principles that might be adopted instead of applying domain or sector specific principles.

The second challenge concerns addressing the variability of privacy as it is subjective in its nature and culturally relative [DFF14, OGD+05]. This variability challenges software engineers to understand and consider stakeholders' expectations and concerns, which, in turn, requires a specific expertise, contextual analysis and resolution of stakeholders' conflict of security and privacy interests [GTD11].

The third challenge concerns the determination of an adequate level of privacy protection without diminishing functionality. This requires applying data minimisation as a foundational principle; however, each software system requires an appropriate type of data minimisation that conforms with its purpose [GTD11]. In addition, there are other considerations that need to be taken into account to determine the appropriate type of data minimisation, such as stakeholders' expectations and concerns, related legislation and an appropriate privacy threat model [SC09].

The fourth challenge concerns the identification and assessment of activities that lead to privacy harms in a comprehensive and meaningful manner. In system engineering, risk assessment goes beyond identifying technical risks of the software system being developed; however, this requires a better understanding of social perceptions and expectations that are derived from social norms [GTD11, DA06]. To some extent, the nature of privacy harms differs from the impact of security events, as the potential impact of privacy violations might

be incorporeal, psychological, or emotional. This means that the negative consequences of privacy violations are not only related to the affected individuals but also may extend beyond that to affect society [Sol06]. In addition, the impact of security risks is often measured from a financial perspective, whereas the impact of privacy risks is measured from two different perspectives: (1) as a financial impact — whether this impact is tangible, such as legal sanctions, or intangible, such as an entity's reputation; and (2) as personal and societal impacts, such as social standing and an individual's reputation [NCM+15]. Furthermore, the economic value of a privacy impact needs to be assessed to determine the level of protection in line with stakeholders' perceptions and expectations [KLL05].

The fifth challenge concerns the appropriate mapping of privacy requirements onto suitable software architectures that support the adequate level of privacy protection. Determining an adequate level of protection challenges software engineers to adopt a useful and rational means to critically reason about the specified level. This includes making appropriate design decisions that fulfil the elicited privacy requirements [GTD11], specifying various levels of privacy protection, and determining appropriate architectural alternatives that support these levels [SC09].

The sixth challenge concerns the assurance of providing full protection of personal data: from collection to destruction. Indeed, developing compliance mechanisms are not sufficient in mitigating privacy concerns that arise throughout the collection and retention of large amount of personal data [GTD11]. This implies that it is crucial to adopt a model that manages the flow of personal data, such as the personal data lifecycle, to support the process of identifying and addressing privacy concerns that arise in each stage of the personal data lifecycle [CMF+10, Can14]. In addition, it is essential to analyse privacy and functional requirements from the early stages of the design process to determine the relevant and necessary data for achieving given functionality [Sch10]. In order to ensure the adequacy, relevance and necessity of personal data, software engineers require a means of supporting the traceability of privacy requirements for each software system's activity.

Having introduced the main challenges of engineering Privacy by Design, we now analyse three privacy requirements engineering methods to understand how these methods address the identified challenges.

2.2 An analysis of existing privacy requirements methods

In this report, we consider three privacy requirements engineering methods: the Framework for Privacy-Friendly System Design (PFSD) [SC09], LINDDUN [DWS+11, WSJ14], and the PriS method [KKG08]. We choose these methods as they were compared in [Bec12], and this comparison was in reference to the conceptual framework for privacy requirements engineering that is proposed by Beckers [Bec12]. In addition, these methods consider different subsets of privacy principles and guidelines as a source of privacy protection goals. However, each method has a different technique for identifying system activities that lead to privacy harms, eliciting privacy requirements and mapping requirements onto software architectures: PFSD focuses on sensitive system operations, LINDDUN concentrates on data flow diagrams, and the PriS method considers business processes. For each method, we analyse how it addresses the challenges of Section 2.1.

2.2.1 The Framework for Privacy-Friendly System Design (PFSD)

The Framework for Privacy-Friendly System Design (PFSD) was developed by Spiekermann and Cranor for engineering privacy [SC09]. Spiekermann and Cranor analyse common privacy definitions and translate these concepts into engineering responsibilities in relation to three different spheres: (1) the user sphere, which consists of the user's devices that they have full control over; (2) the recipient sphere, which consists of the data holder's infrastructure, in which a user does not have control over their personal data; and (3) the joint sphere, which consists of the data holder's infrastructure that hosts individuals' personal data and provides additional services, such as email services, which provides users access to their personal data, over which they expect to have control. These responsibilities address two main issues. First, users should be provided with access to exercise control over their personal data. Second, privacy risks should be mitigated where personal data is not under users' control. As a result, a high level privacy responsibility framework was developed to serve as a basis for requirements analysis and elicitation. Furthermore, Spiekermann and Cranor emphasise the importance of understanding users' privacy expectations and concerns in a contextual manner. Thus, the PFSD framework defines a three-layer model that explains a set of static concerns that were identified as a result of empirical studies [SMB96] in relation to three sensitive system operations, i.e. data transfer, data storage and data processing. However, identifying a set of static concerns is not sufficient to address the variability of privacy, as privacy perceptions are influenced by legal, social and economic changes as well as technology advancements. In addition, the PFSD framework adopts the Federal Trade Commission (FTC) privacy principles [Uni10]. These principles are a subset of the Organisation for Economic Co-operation and Development (OECD) guidelines [Org13]. By adopting these principles, Spiekermann and Cranor aim to implement specific mechanisms for notice, choice, access, and compliance enforcements, such as audit and policy enforcement. Furthermore, the PFSD framework adopts unlinkability, transparency and intervenability as privacy protection goals. It is understandable that the PFSD framework is likely to be domain-specific for e-commerce and ubiquitous computing [SC09].

Furthermore, the PFSD framework identifies system activities that lead to privacy harms by analysing functional requirements, and privacy expectations and concerns. The potential impact is estimated based on several factors, i.e. types of personal data, the way these operations are performed and the domain in which the data is processed. In spite of adopting a static set of privacy concerns, limiting the analysis to three system operations is not sufficient in identifying potentially harmful activities in a comprehensive manner. Other considerations need to be taken into account, such as the flow of personal data among involved actors together with their roles and responsibilities, whether those actors are in the same entity or third parties. In addition, the PFSD framework emphasises the importance of considering appropriate threat models to specify the acceptable level of privacy protection. However, it does not explicitly adopt a specific privacy risk analysis and assessment processes, as well as models that aid managing the flow of personal data and guide the identification of potential privacy harms in each stage of the personal data lifecycle to ensure full protection of privacy [SC09].

In addition, the PFSD framework identifies a set of criteria for specifying the degree to which privacy is required, i.e. privacy expectations, legal requirements, appropriate threat

models and technological capabilities. Based on those criteria together with business and technical strategies, software engineers can adopt one of the proposed approaches. The first approach is privacy-by-policy, which concentrates on enforcing privacy policies during personal data processing by implementing enforcement and compliance mechanisms. The second approach is privacy-by-architecture, which focuses on architectural choices by applying the principle of data minimisation as a foundational step for engineering software systems. These approaches are accompanied by guidelines that aid software engineers in selecting appropriate architectural alternatives that are adequate for various levels of privacy protections based on the degree of identifiability and linkability of personal data. These choices reflect the degree to which privacy is required in a four-level scale: from identified and linked to anonymous and unlinkable personal data [SC09].

2.2.2 LINDDUN

LINDDUN is a privacy threat analysis framework for supporting the elicitation and fulfilment of privacy requirements. It provides a set of privacy threat types and a means for mapping these threat types to the elements of a Data Flow Diagram (DFD). The identified threat types are Linkability, Identifiablitiy, Non-repudiation, Detectability, Disclosure of information, content Unawareness, and policy and consent Non-compliance. The name of this framework (LINDDUN) is derived from these threat types [DWS+11, WSJ14].

LINDDUN adopts a set of privacy protection goals rather than referring to particular concepts, principles and guidelines of privacy. It considers seven privacy protection goals, i.e. unlinkability, anonymity and pseudonymity, undetectability and unobservability, plausible deniability, confidentiality, content awareness, and policy and consent compliance. These protection goals are in line with the terminology proposed by Pfitzmann et al. [PH10]. The method emphasises the variability of privacy as a subjective concept; however, it does not explicitly illustrate how to address this variability in relation to social expectations in each particular context.

The method identifies potentially harmful activities by providing threat tree patterns as a catalogue, which simplifies the identification process by providing possible vulnerabilities for each threat. From these patterns, misuse cases are derived and documented, and requirements are elicited. The identified threats are mitigated by adopting the principle of data minimisation as a fundamental step in privacy protection, which supports specifying various levels of privacy protection based on the protection goals. However, threat tree patterns need to be continuously updated to consider new threats. In addition, LINDDUN is independent from any particular privacy risk analysis and assessment processes. This independence gives software engineers the opportunity to adopt familiar privacy risk methodology. Furthermore, the method adopts Data Flow Diagrams (DFDs) to represent a high level of abstraction of the system that guides software engineers to identify where privacy threats may occur during the flow of personal data. However, to ensure identifying possible activities that lead to privacy harms in a comprehensive manner, the personal data lifecycle needs to be considered in relation to the elements of the Data Flow Diagrams to avoid harmful activities that may have potential impacts on privacy, such as data collection methods [DWS+11, WSJ14].

In addition, LINDDUN supports the interaction between privacy requirements and soft-

ware architectures by providing a catalogue of threat tree patterns that aids software engineers in mapping appropriate Privacy-Enhancing Technologies (PETs) onto the identified threat types [DWS+11, WSJ14].

2.2.3 The PriS Method

The PriS method is a requirements engineering method that aims to integrate privacy requirements into the early stages of the design process by modelling privacy requirements as organisational goals [KKG08]. The method emphasises the complexity of privacy as a legal and social concept. However, it considers eight privacy requirements as privacy protection goals rather than referring to specific privacy definitions, principles and guidelines, These protection goals are identification, authentication, authorisation, data protection, anonymity, pseudonymity, unlinkability and unobservability. In particular, some security goals may have implications on privacy, therefore, identification, authentication and authorisation, as security services, are adopted together with privacy protection goals. The aim of such goals is to eliminate or minimise the collection and processing of personal data according to the relevant privacy legislation. In addition, the method considers stakeholders' expectations and concerns during the elicitation of privacy related goals in relation to the environment in which the software system operates. This is accomplished by stakeholders' participation in respect of the eight privacy protection goals. Each goal has relevant stakeholders who may have different conflicts of interest; therefore, conflict resolution techniques can be used to resolve these conflicts to support the achievement of other goals [KKG08].

Having elicited privacy related goals, the impact of privacy goals on processes and their supporting software systems is analysed. This may lead to the identification of new goals, which lead to new processes, or improve existing goals, which lead to improve existing processes. Then, these processes are modelled using relevant privacy-process patterns, which are generic process models that consist of several activities and flows to illustrate the relationships among them, and represent how business processes are executed in a particular domain. However, the method does not adopt specific risk identification, analysis and assessment processes. Furthermore, the PriS method adopts goal models to guide software engineers in addressing privacy concerns in each process. However, it is understandable that the method considers analysing business processes and their supporting software systems instead of modelling the flow of personal data. As a consequence, this level of abstraction affects the identification of certain harmful activities that arise in each stage of the data lifecycle in a comprehensive manner, such as collection methods in the collection stage [KKG08].

In addition, the PriS method supports the mapping of privacy requirements onto appropriate software architectures by providing privacy-process patterns. Each pattern illustrates privacy activities that need to be implemented, which, in turn, aids software engineers in deciding where privacy controls, i.e. Privacy-Enhancing Technologies (PETs), need to be implemented to achieve an acceptable level of privacy protection. Furthermore, alternative architectural choices can be prioritised according to the degree to which privacy is required to provide various levels of privacy protection [KKG08].

2.2.4 Summary

Table 1 shows the result of the analysis of the three privacy requirements methods in reference to the challenges of Section 2.1. In the analysis, we focus on how these methods address the main challenges of engineering Privacy by Design. A table entry labelled with "*" means the method addresses this challenge, a table entry labelled with "-" means the method partially addresses this challenge, and an empty space means that the method does not explicitly address this challenge.

The analysed methods adopt various sets of privacy protection goals rather than referring to standard privacy principles and guidelines. This implies that there is no consensus on a standard set of protection goals to be used in various contexts. It is understandable that some methods are applicable to specific domains. From an engineering perspective, however, it is practical to adopt a universal standard of privacy principles from which a set of privacy protection goals can be derived to be used in a variety of contexts. In addition, none of these methods thoroughly address the complexity and variability of privacy by focusing on harmful activities that may disrupt stakeholders' expectations. This, however, requires understanding stakeholders' expectations and concerns in a contextual manner. Furthermore, none of these methods explicitly adopt specific impact analysis and assessment processes, which, in turn, gives software engineers the opportunity to adopt familiar processes. In respect of specifying the adequate level of privacy protection, only the PFSD framework defines various levels based on two explicit criteria: identifiability and linkability of personal data. However, other methods implicitly consider that the adequate level of protection depends on design decisions. In addition, none of these methods apply the personal data lifecycle explicitly; rather they apply different models that represent some stages of the personal data lifecycle at a high level of abstraction, such as Data Flow Diagrams (DFDs) and Business Process Model. In addition, it is noticeable that the analysed methods provide different means for mapping privacy requirements onto software artefacts, such as catalogues and process-patterns. From an engineering perspective, however, catalogues and patterns alone are not sufficient for software engineers to reason critically about design decisions.

Challenges	**PFSD**	**LINDDUN**	**PriS**
Universal privacy principles and protection goals	-		
Appropriate interpretation of privacy perceptions	-		-
Potential impact analysis and assessment			
Multi-levels of privacy protection	*	-	-
The adoption of the personal data lifecycle	-	-	-
Means for mapping requirements onto architecture	*	*	*

Table 1: The identified challenges in relation to the three analysed methods

2.3 A set of criteria for engineering Privacy by Design

Having explained the main challenges of engineering Privacy by Design in Section 2.1, and analysed three privacy requirements engineering methods in Section 2.2, we now derive a set of criteria that support the process of engineering Privacy by Design to address these challenges.

2.3.1 The adoption of universal privacy principles and protection goals

The aim of this criterion is to emphasise the importance of adopting a unified set of privacy principles that are derived from the Fair Information Practice Principles (FIPPs). By adopting such principles, universal and comprehensive privacy protection goals and objectives can be specified and agreed to be applied in a variety of contexts in various jurisdictions. In particular, the global privacy standard (GPS) [Cav06] harmonises various sets of the Fair Information Practice Principles (FIPPs) into universal privacy principles [Cav10]. Thus, the foundational principles of Privacy by Design are based on the GPS privacy principles [Cav10]. Since these principles are in line with privacy legislation and data protection regulations, they can be adopted in the context of privacy engineering. It is understandable that in some jurisdictions data protection regulations are sectoral models, such as healthcare and financial services. Therefore, these regulations can be adopted as transmission principles during the contextual analysis, as will be further explained in the following sections.

In order to achieve privacy principles, a set of universal privacy protection goals need to be specified to identify the rights of data subjects and the obligations of entities with reference to the global privacy standard principles [Cav06]. Such protection goals need to be much broader than data minimisation to achieve all privacy principles and address the complexity and variability of privacy as a legal, social and political concept. In privacy literature, Hansen et al. [HJR15] emphasise six protection goals for privacy engineering as a basis from which software engineers can derive privacy requirements, select appropriate technologies that fulfil these requirements, and assess the impact of privacy in a given software system. These protection goals were already proposed by [Han11, RB11], while privacy-related protection goals were also defined by [PKK01, PH10]. However, three of these six goals are confidentiality, integrity, and availability, which are commonly thought of as the main properties of security. Indeed, security has been recognised to support privacy engineering [HJR15]; however, we assume that security properties and services are taken into account during the design process to support privacy in achieving an adequate level of privacy protection. This means that we will leverage the other three goals, which are unlinkability, transparency and intervenability as privacy protection goals. In more detail, we consider unlinkability as a general goal and its specific properties, i.e. anonymity, undetectability and unobservability, and pseudonymity.

To map these protection goals onto the principles of the global privacy standards [Cav06], unlinkability, as a protection goal, and its specific properties can be mapped onto data minimisation as a main concept of the *collection limitation principle*, which, in turn, is related to other principles, i.e. *purposes, use, retention, and disclosure limitation*. This protection goal is derived directly from privacy regulation articles [HJR15]. In addition, transparency, as a protection goal, can be mapped onto the principle of *openness*, as it is

a prerequisite for accountability. This protection goal is required by the new proposal of the EU Data Protection Directive [HJR15]. Furthermore, intervenability, as a protection goal, can be mapped onto the principles of *consent, access, accuracy and compliance*. This protection goal is directly derived from the regulation articles such as consent [HJR15].

In respect of existing methods, LINDDUN adopts *content awareness*, and *policy and consent compliance* as protection goals; therefore, these goals are partially related to transparency and intervenability [HJR15]. Other protection goals are related to confidentiality and unlinkability. In addition, the data minimisation principle has a vital role in achieving an adequate level of privacy protection; however, it falls short when data disclosure is reasonably required [HJR15]. The PriS method considers eight privacy protection requirements: identification, authentication, authorisation, data protection, anonymity, pseudonymity, unlinkability and unobservability [KKG07, KKG08]. However, the three protection requirements are security services, whereas, data protection, as a requirement, is related to the data protection rules and regulations. This means that data protection, as a protection goal, is highly abstracted and comprises several protection goals. In addition, the PriS method highlights anonymity, pseudonymity, unlinkability and unobservability as protection requirements, whereas they are already demanded by data protection whether in a direct or indirect way, such as via data minimisation. The PFSD framework adopts the Fair Information Practice Principles (FIPPs) that have been developed by the Federal Trade Commission (FTC). In addition, it considers anonymity and pseudonymity as specific properties of unlinkability, which is a general protection goal. In summary, these goals are identified to express stakeholders' privacy concerns towards their personal data.

2.3.2 The adoption of the data lifecycle as a basis for the contextual analysis to identify system harmful activities in a comperhensive manner

The aim of this criterion is to support the process of identifying and addressing activities that lead to privacy harms that arise in each stage of the personal data lifecycle in a comprehensive and concrete manner. The personal data lifecycle, as a model, guides software engineers in evaluating the flow of personal data [CMF+10, Can14], as well as tracing privacy requirements of the software system being developed to ensure compliance with privacy principles in each stage. In addition, it can be used as a means to facilitate communication between various stakeholders, such as policymakers, data protection authorities' representatives, data subjects' representatives, software engineers, and senior management, by providing a common language. In particular, privacy principles are written in a way to govern and regulate processing of personal data in each stage of the data lifecycle. In respect of the analysed methods, the personal data lifecycle is not adopted explicitly. Instead, these methods apply models that represent some stages of the personal data lifecycle at a high level of abstraction, such as Data Flow Diagrams (DFDs) and Business Process Model to identify potentially harmful activities.

2.3.3 The appropriate interpretation of stakeholders' expectations and concerns into operational requirements

The aim of this criterion is to address the complexity and variability of privacy by translating social, legal and political perceptions, expectations and concerns into operational requirements in a contextual manner. This can be achieved by considering harmful activities that have implications on privacy rather than referring to abstract definitions [Sol06]. In particular, Solove's taxonomy of privacy [Sol06] illustrates all kinds of such activities around a model that represents the flow of personal data. The taxonomy can be adopted to aid software engineers in identifying software system activities that lead to privacy harms in a concrete manner. In addition, the contextual integrity framework [Nis09] can be adopted to aid software engineers in understanding stakeholders' expectations and concerns in each particular context. In so doing, appropriate privacy perceptions can be understood in a non-reductive and concrete manner. In respect of the analysed methods, the PFSD framework considers a set of static concerns as a result of empirical studies. However, these concerns vary in various contexts and may change over time, as privacy is subjective in its nature and depends on the culture and expectations of each society [OGD+05]. To achieve legal compliance and get a better acceptance of a given software system, other stakeholders' expectations and concerns need to be considered, such as data protection authorities, policymakers, senior management and so forth.

2.3.4 The adoption of an appropriate privacy threat analysis framework accompanying by impact analysis and assessment processes

The aim of this criterion is to identify system activities that lead to privacy harms in a comprehensive, concrete and contextual manner. This can be achieved by synthesising the taxonomy of privacy harms [Sol06] and the contextual integrity framework [Nis09] to understand reasonable expectations and refer to them as a baseline during the analysis process. In addition, the personal data lifecycle can be used as a basis for the identification of process to aid software engineers in addressing privacy concerns that may arise in each stage of the personal data lifecycle. In order to make rational treatment decisions, appropriate impact analysis and assessment processes need to be adopted, such as the Privacy Risk Management (PRM) [CMF+10] and the Methodology for Privacy Risk Management [Com16], which were developed based on the ISO 31000 Risk Management Framework [ISO09]. Such frameworks estimate the level of materialised privacy risks according to the causes of the identified adverse privacy events and their potential impacts. In doing so, software engineers can holistically identify and systematically analyse privacy risks to elicit concrete privacy requirements [GTD11]. In respect of the analysed methods, potentially harmful activities are identified in different processes. In particular, the PFSD framework identifies privacy concerns by analysing sensitive operations in relation to the three spheres of influence. In addition, LINDDUN identifies privacy concerns by mapping privacy threats into the main elements of a data flaw diagram, whereas the PriS method analyses the impact of privacy goals on business processes and their associated software systems.

2.3.5 The specification of the required level of privacy protection

The aim of this criterion is to determine the adequate level of privacy protection that is required for the software system being developed. This level is based on a number of factors: stakeholders' expectations and concerns, appropriate threat models, relevant legislation, technological capabilities and appropriate types of data minimisation [SC09]. In particular domains, users' expectation may exceed related legal requirements. Therefore, this criterion aims to identify multi-levels of privacy protection, i.e. the default settings can be the maximum level of privacy protection [Cav10] and other levels can be specified by considering data subjects' preferences [BBK+12]. This means that to address the variability of privacy, reasonable expectations of various stakeholders need to be considered at an architectural level. Of the ones surveyed, however, only the PFSD framework explicitly defines four levels of privacy protection, whereas others leave this to software engineers to apply technical measures that achieve an acceptable level of privacy protection.

2.3.6 The identification of appropriate strategies for mapping privacy requirements onto software architectures

The aim of this criterion is to support the interaction between privacy requirements and software architectures. This can be achieved by identifying design strategies that aid software engineers in translating privacy requirements into software architectural decisions. In addition, strategies aid software engineers in specifying the adequate level of privacy protection in a reasoned and effective manner, justifying applied technical measures and arguing critically about design decisions. Such strategies can be used as a basis for identifying useful architectural patterns, corresponding design patterns and underlying Privacy-Enhancing Technologies (PETs). Furthermore, strategies can be used as objectives or support for achieving privacy protection goals. In respect of the analysed methods, the PFSD framework applies the principle of data minimisation in relation to the three technical domains to specify appropriate architectural choices that fulfil privacy requirements, whereas LINDDUN and the PriS methods use catalogues and privacy-process patterns respectively to determine appropriate technical measures. However, catalogues and patterns alone are not sufficient for software engineers to reason critically about adopting particular technologies or making critical design decisions. This, in turn, requires identifying means that illustrate appropriate conditions for adopting each architectural pattern, design pattern and underlying technologies in relation to the adequate level of privacy protection in each particular context.

2.4 Summary

In the proceeding subsections, we explored the main challenges of engineering Privacy by Design and analysed three privacy requirements methods to understand how those methods address the main challenges. Subsequently, we derived a set of criteria that address these challenges and support the process of engineering Privacy by Design. These criteria emphasise the importance of developing an appropriate privacy threat analysis framework that adopts universal privacy principles from which privacy protection goals are derived to

express stakeholders' privacy concerns towards their personal data. Such a framework needs to be complemented by impact analysis and assessment processes to identify and address potentially harmful activities in a holistic and systematic manner. The framework needs to identify a number of factors for specifying multi-levels of privacy protection that address privacy concerns and meet stakeholders' expectations. Furthermore, the framework needs to support the interaction between the analysis and design phases by identifying design strategies as objectives for achieving the privacy protection goals. These strategies, indeed, play a vital role in mapping privacy requirement onto software architectures, which, in turn, aid software engineers to apply appropriate architectural patterns and their underlying technologies. Last but not least, an appropriate privacy threat analysis framework is considered to be a fundamental step in identifying system activities that lead to privacy harms, conducting an impact analysis and assessment processes, eliciting privacy requirements, and specifying design decisions that fulfil these requirements at an architectural level.

3 Privacy by Design: an analysis in respect of the identified criteria

In this section, we will analyse the foundational principles of Privacy by Design in respect of the identified criteria in Section 2.3. As mentioned previously, the aim of these criteria is to confront the challenges of Section 2.1 and support the process of engineering Privacy by Design.

3.1 The foundational principles of Privacy by Design

The foundational principles of Privacy by Design are based on the Fair Information Practice Principles (FIPPs) [Uni73], and extend beyond these principles to act as a comprehensive and universal framework for integrating privacy and data protection effectively and proactively into information and communication technologies, business practices, and physical design and infrastructures to meet legal obligations, achieve accountability and enhance user trust [Cav10, CSC14].

In particular, these principles are based on the global privacy standard [Cav10], which harmonises various sets of the Fair Information Practice Principles (FIPPs) into universal privacy principles [Cav10]. The global privacy standard, as a set of principles, was accepted at the 28th International Data Protection and Privacy Commissioners Conference [Cav06]. It is noteworthy that the global privacy standard explicitly distinguishes the concept of data minimisation in the principle of collection limitation [Cav06].

3.1.1 Proactive not Reactive; Preventative not Remedial

This principle aims to emphasise the main characteristics of the Privacy by Design approach. These include identifying and addressing privacy concerns in a proactive, systematic, and creative manner [Cav10].

To achieve the aim of this principle, a holistic, proactive and systematic approach needs to be devised to identify system activities that lead to privacy harms at the early stages

of the design process [Cav10]. Such an approach needs to be complemented by impact analysis and assessment processes. To be a holistic approach, the identification of potentially harmful activities needs to be done in a comprehensive, concrete and contextual manner. In order to meet stakeholders' expectations, which often extend beyond legal requirements in some contexts and jurisdictions [Cav10, Bec12], high standards of privacy need to be adopted and enforced [Cav10]. To be a proactive, systematic and creative approach, impact analysis and assessment processes need to be adopted, such as Privacy Impact Assessment (PIA). PIA, as a systematic tool, is expected to identify privacy concerns and mitigate their potential impacts by applying privacy measures, whether these measures are technical or administrative [Cav10]. In practice, however, technical progress often introduces new implications on privacy [BBK+12]. Therefore, Wright [Wri12] argues that a PIA is not only a systematic tool, but it is also an ongoing process. Wright, therefore, defines a PIA as a methodology of assessment to identify all potential privacy impacts, and mitigate these impacts as an ongoing process with stakeholders' participation. This implies that a PIA needs to be complemented by robust threat analysis framework and impact analysis process to achieve its goals [CSC14].

Thus, this principle is in line with the first criterion (Section 2.3.1), as the adoption of universal privacy principles provides high standards of privacy that may exceed legal requirements in some jurisdictions. Furthermore, this principle is in line with the third criterion (Section 2.3.3), as appropriate interpretation of stakeholders' expectations and concerns supports eliciting concrete privacy requirements in a holistic manner. In addition, this principle is in line with the fourth criterion (Section 2.3.4), as the adoption of an appropriate threat analysis framework, which is complemented by impact analysis and assessment processes, supports the identification and mitigation of potentially harmful activities in proactive, systematic, and creative manners.

3.1.2 Privacy as the Default Setting

This principle aims to provide a high level of privacy protection as a default setting, i.e. Privacy by Default [Cav10]. In particular, privacy as the default setting is considered as a system property [BBK+12]. 'Privacy as the Default Setting' emphasises a subset of the Fair Information Practice Principles (FIPPs) in respect of purpose specification, collection limitation, data minimisation, and use, retention and disclosure limitation. [Cav10].

'Privacy by Default' implies that the default setting is considered as the adequate level of privacy protection. In practice, however, users are not likely to restrict themselves by a default operational mode, as the functionality of a given software system was designed according to the foundational principles of Privacy by Design [BBK+12]. In essence, any additional privacy features need to be designed according to the foundational principles, whether or not these features are available in the default operational mode [BBK+12]. From a technical perspective, privacy features need to be 'hierarchically nested' in each component of a given software system, to be stimulated by the 'informed consent' of the data subject. This, in turn, supports software evolution and maintenance [BBK+12]. To specify the adequate level of privacy protection as the default setting, the principle of data minimisation with reference to purpose specification, collection, use, retention and disclosure limitation needs to be applied to specify the appropriate type of data minimisation. This,

in turn, requires conducting a contextual analysis to understand and meet stakeholders' expectations and concerns, adopting appropriate threat models to identify activities that lead to privacy harms, and conduct impact analysis and assessment to specify the adequate level of privacy protection as the default setting.

Thus, this principle is in line with the third criterion (Section 2.3.3), as appropriate interpretation of stakeholders' expectations and concerns into systems requirements is a prerequisite of specifying the adequate level of privacy protection. In addition, this principle is in line with the fourth criterion (Section 2.3.4), as the adoption of an appropriate threat analysis framework, which is complemented by impact analysis and assessment processes, supports the specification of the adequate level of privacy protection by identifying and addressing harmful activities that lead to privacy harms that may arise in each level of protection. Furthermore, this principle is in line with the fifth criterion (Section 2.3.5), as the specification of the adequate level of privacy protection can be enforced to be the default setting.

3.1.3 Privacy Embedded into Design

This principle aims to integrate privacy requirements into the design and architecture of software systems, business practices and physical design. This integration needs to be in a holistic, integrative and creative manner [Cav10]. To achieve the aim of this principle, a systematic and principled approach that is built on universal privacy principles and standards needs to be devised to achieve this integration [Cav10]. In more detail, this approach needs to be holistic to consider a variety of contexts, integrative to encourage stakeholders' participation, and creative to invent acceptable design choices. In addition, this approach needs to be complemented by impact analysis and assessment processes to document and communicate the results of the analysis to stakeholders [Cav10]. To ensure the adequate level of privacy protection, a privacy impact assessment needs to be undertaken at each stage or iteration of the engineering process [BBK+12]. However, a pragmatic method of evaluating the positive-sum needs to be clearly defined to ensure that embedding privacy does not diminish the functionality of a given software system [BBK+12].

Thus, this principle is in line with the third criterion (Section 2.3.3), as appropriate interpretation of stakeholders' expectations and concerns supports eliciting concrete privacy requirements in a holistic manner. In addition, this principle is in line with the fourth criterion (Section 2.3.4), as the adoption of an appropriate threat analysis framework, which is complemented by impact analysis and assessment processes, supports the determination of the adequate level of privacy protection. Furthermore, this principle is in line with the sixth criterion (Section 2.3.6), as the identification of appropriate strategies for mapping privacy requirements onto software architectures supports making architectural choices that implement the adequate level of privacy protection in a creative and positive-sum manner. Additionally, these three criteria support devising the demanded approach by this foundational principle [Cav10].

3.1.4 Full Functionality - Positive-Sum, not Zero-Sum

This principle aims to achieve all privacy interests and entities' objectives in a positive-sum manner [Cav10]. To achieve the aim of this principle, privacy requirements need to be embedded in a creative manner without affecting other software system properties and attributes [Cav10]. However, the adequate level of privacy protection and the functionality of a given software system need to be measured to assess whether they are in a positive-sum or a zero-sum relationship [BBK+12]. This means that functionality and privacy requirements need be prioritised and weighted in a systematic manner. In reality, however, it is a challenge to weigh these requirements, and some research needs to be conducted in this regard [BBK+12]. This, in turn, needs a clear assessment method to ensure the result of the trade-off between privacy and functionality is in a positive-sum [BBK+12]. In general, legitimate interests and objectives are reflected by functional requirements that are constrained by stakeholders' expectations and concerns. However, software systems have become increasingly large and complex, thus, software architectures are considered effective tools to manage the complexity of large-scale software systems from a high level of abstraction, and from both technical and managerial perspectives [CSXM09]. This means that software architecture is considered to be a place for innovative and creative choices, and can be analysed and evaluated to achieve all system properties and quality attributes.

Thus, this principle is in line with the third criterion (Section 2.3.3), as appropriate interpretation of stakeholders' expectations and concerns supports the analysis and prioritisation of functional requirements. In addition, this principle is in line with the fourth criterion (Section 2.3.4), as the adoption of an appropriate threat analysis framework, which is complemented by impact analysis and assessment processes, supports the determination of the adequate level of privacy protection. Moreover, this principle is in line with the fifth criterion (Section 2.3.5), as the specification of the adequate level of privacy protection is considered to be the highest level of protection. Furthermore, this principle is in line with the sixth criterion (Section 2.3.6), as the identification of appropriate strategies for mapping privacy requirements onto software architectures supports making architectural choices that implement the adequate level of privacy protection in a creative, innovative and positive-sum manner.

3.1.5 End-to-End Security - Full Lifecycle Protection

This principle aims to protect personal data throughout the entire lifecycle from collection to destruction by implementing strong security measures [Cav10]. 'Full Lifecycle Protection' emphasises security as a principle of the Fair Information Practice Principles (FIPPs) [Cav10]. However, measuring the level of security of complex software systems is a challenge [BBK+12]. Security is a process, which means that technical controls are not sufficient, and social factors need to be considered for providing adequate data protection, i.e. people's behaviour during the process [BBK+12]. To achieve the aim of this principle, the personal data lifecycle needs to be considered as a basis for the identification of activities that lead to privacy harms, impact analysis and assessment. The impact analysis and assessment processes need to complement an appropriate threat analysis framework to identify and address privacy concerns that arise in each stage of the lifecycle with stakeholders'

participation to meet their expectations and concerns.

Thus, this principle is in line with the third criterion (Section 2.3.3), as appropriate interpretation of stakeholders' expectations and concerns supports determining appropriate types of data minimisation in reference to purpose specification, use, retention, disclosure and destruction limitation. In addition, this principle is in line with the fourth criterion (Section 2.3.4), as the adoption of an appropriate threat analysis framework, which is complemented by impact analysis and assessment processes, supports the determination of the adequate level of privacy protection. Furthermore, this principle is in line with the sixth criterion (Section 2.3.6), as the identification of appropriate strategies for mapping privacy requirements onto software architectures supports making architectural choices that implement the adequate level of privacy protection in a creative and positive-sum manner. Additionally, this principle is in line with the second criterion (Section 2.3.2), as the adoption of the data lifecycle as a basis for the contextual analysis supports the identification, mitigation and tractability of privacy concerns that arise in each stage of the lifecycle with stakeholders' participation to meet their expectations and concerns.

3.1.6 Visibility and Transparency - Keep it Open

This principle aims to assure all stakeholders that personal data is processed in relation to the specified purposes and is subject to independent verification [Cav10]. 'Keep it open' emphasises a subset of the Fair Information Practice Principles (FIPPs) in respect of accountability, openness, and compliance, which, in turn, improve user satisfaction and trust [Cav10]. Visibility and transparency are prerequisites for accountability, and can be achieved by implementing compliance mechanisms, such as notice, access mechanisms and audit trails. In particular, adequate privacy polices that precisely define compliance rules need to be specified, documented and communicated [Cav10]. This means that compliance rules should be integrated with privacy requirements to achieve a satisfied level of accountability and user satisfaction. In addition, privacy protection goals need to be specified and documented to be used as a reference for all design decisions [BBK+12]. From a technical perspective, transparency can be achieved by the traceability of personal data throughout the data lifecycle [BBK+12].

Thus, this principle is in line with the first criterion (Section 2.3.1), as the adoption of universal privacy principles embody accountability, openness, and compliance, which can be achieved by specifying, documenting and communicating privacy protection goals and objectives to various stakeholders. In addition, this principle is in line with the second criterion (Section 2.3.2), as the adoption of the data lifecycle as a basis for the contextual analysis supports the tractability of privacy requirements to ensure compliance in each stage of the lifecycle. This, in turn, achieves accountability by implementing various mechanisms that meet regulatory compliance and stakeholders' expectations and concerns.

3.1.7 Respect for User Privacy - Keep it User-Centric

This principle aims to ensure that software architects, designers and operators are aware of data subjects' privacy expectations [Cav10]. This can be achieved by providing privacy measures, such as a default setting, appropriate notice and user-friendly features [Cav10]. 'Keep

it User-Centric' emphasises a subset of the Fair Information Practice Principles (FIPPs) in respect of consent, accuracy, access and compliance [Cav10].

This principle emphasises the interaction between the data subject and a software system. However, privacy is subjective in its nature and depends on the culture and expectations of each society [OGD+05]. Therefore, this interaction needs to be in conformance to stakeholders' expectations and concerns. This leads to the importance of considering the expectations of various stakeholders, specifically, data subjects [BBK+12]. To empower the data subject, consent and privacy preferences need to be considered, and data avoidance needs to be an option rather than providing one level of privacy protection as a default setting. By applying data avoidance as a default setting, the data subject cannot exercise the right of informational self-determination. Accordingly, Bier et al. [BBK+12] propose that this principle can be achieved by designing configurable privacy features. In addition, potential alternatives for implementing each privacy feature need to be interchangeable in a modular manner [BBK+12]. Then, the configuration of a specific privacy feature needs to be adaptable for each data subject [BBK+12].

Thus, this principle is in line with the third criterion (Section 2.3.3), as appropriate interpretation of stakeholders' expectations and concerns addresses the variability of privacy by meeting various stakeholders' expectations. In addition, this principle is in line with the fourth criterion (Section 2.3.4), as the adoption of an appropriate threat analysis framework, which is complemented by impact analysis and assessment processes, supports the determination of the adequate level of privacy protection, as each alternative that implements a set of privacy preferences involves different kinds of harmful activities. Furthermore, this principle is in line with the fifth criterion (Section 2.3.5), as the specification of the adequate level of privacy protection can be enforced as the default setting. Additionally, this principle is in line with the sixth criterion (Section 2.3.6), as the adoption of appropriate means for mapping privacy requirements onto software architectures supports making architectural choices that implement multi-levels of privacy protection in a creative and positive-sum manner with stakeholders' participation to meet their expectations and concerns.

3.2 Summary

Privacy by Design aims to incorporate privacy requirements into the early stages of the design process to meet legal obligations, achieve accountability and enhance user trust. However, its foundational principles are given at a high level of abstraction, which, in turn, introduces a number of challenges in terms of integrating this approach into systems engineering. By analysing these principles, the derived criteria are in line with the foundational principles and support the translation of these principles into engineering activities to achieve the aims of Privacy by Design in the context of software-based systems. In particular, each foundational principle can be achieved by embodying one or more of these criteria that are intended to address the main challenges and integrate the foundational principles into the engineering process.

Having analysed the foundational principles of Privacy by Design in respect of the derived criteria, in Section 4 we will illustrate in more detail a proposal towards a principled approach for engineering Privacy by Design. The proposed approach is intended to complement the

Privacy by Design approach and fill in the gaps.

4 A proposal: towards a principled approach for engineering Privacy by Design

In the preceding sections, we explained the main challenges of engineering Privacy by Design, analysed three methods of privacy requirements elicitation, and derived a set of criteria to address these challenges. In this section, we present a proposal towards a principled approach, which will be developed in reference to the identified criteria that support the process of engineering Privacy by Design. The proposed approach is intended to complement Privacy by Design and can be used as a means for addressing the limitations of appropriate adoption of the Privacy by Design approach.

4.1 The proposed approach

In more detail, the proposed approach is intended to be in consonance with the foundational principles of Privacy by Design and their underlying Fair Information Practice Principles (FIPPs) for embedding privacy requirements into the early stages of the design process. The main elements of the proposed approach are as follows.

1. **Universal privacy principles and protection goals.** The global privacy standard (GPS) [Cav06] harmonises various sets of the Fair Information Practice Principles (FIPPs) into universal privacy principles [Cav10]. Thus, the foundational principles of Privacy by Design are based on the GPS privacy principles [Cav10]. In the proposed approach, we adopt the global privacy standard as a set of universal privacy principles to be applied in a variety of contexts in various jurisdictions. To achieve these principles, we adopt unlinkability, transparency and intervenability as a set of privacy protection goals that are proposed by [HJR15] to complement security protection goals, i.e. confidentiality, integrity and availability.

2. **The personal data lifecycle.** In the context of privacy and data protection, typically, the personal data lifecycle consists of five stages: data collection, retention, use, disclosure, and destruction. On the one hand, each stage of the data lifecycle has a set of principles that govern the processing of personal data. For example, collection limitation and purpose specification are privacy principles that govern personal data at the collection stage. On the other hand, each stage has certain concerns and associated harmful activities that have implications on data subjects' privacy. To achieve a full level of privacy protection, the data lifecycle is considered to be a foundational step in the proposed approach to support the identification, mitigation and traceability of privacy concerns that arise in each stage of the lifecycle in a holistic and integrative manner. In essence, it is considered as a basis for the contextual analysis.

3. **A synthesised privacy threat analysis framework.** This framework attempts to bridge the gap between policymakers and software engineers by synthesising two

existing frameworks to appropriately interpret privacy perceptions and identify potentially harmful activities. The first is the taxonomy of privacy [Sol06], which was developed from a legal perspective around a model that represents the flow of personal data to understand activities that lead to privacy harms in a comprehensive and concrete manner. The second is the contextual integrity framework, which was developed from social and philosophical theories to understand privacy expectations and their implications [Nis09]. By synthesising such frameworks, legal, social and political perceptions can be translated into operational requirements to be reconciled with system requirements in a structured manner.

In practice, processing personal data may present various privacy risks, which have potential impacts on data subjects as well as entities whether this impact is tangible, such as legal sanctions, or intangible, such as an entity's reputation. Therefore, this framework needs to be complemented by impact analysis and assessment processes to support structured reasoning about identifying and addressing potentially harmful activities. In this context, personal data is the valuable asset that needs to be protected. This, in turn, aids software engineers in eliciting concrete privacy requirements and specifying appropriate designs at an architectural level.

In essence, a privacy risk is composed of an adverse event and all threats that make it possible by successfully exploiting vulnerabilities of a given software system. In the following sections, we will explain how adverse events, vulnerabilities and threats are identified as well as how a privacy risk is estimated.

(a) **An adverse event.** An adverse event is characterised as the effect or influence of a harmful activity on the privacy of a data subject. This effect or influence needs to be avoided or at least reduced to an acceptable level. In this framework, we adopt the taxonomy of privacy [Sol06] as a useful source of identifying adverse events that may occur in each stage of the personal data lifecycle. For example, insecurity as an adverse event involves harmful activities that result from: '*carelessness in protecting stored information from leaks and improper access*' [Sol06], and its potential impact is: '*the injury of being placed in a weakened state, of being made more vulnerable to a range of future harms*' [Sol06], which indicates that a lack of security measures supports threats that make it possible. In particular, harmful activities are considered as adverse events as well as indicators of their negative consequences as privacy harms. Indeed, the occurrence of such events has implications on the privacy of data subjects.

In summary, an adverse event describes possible harmful activities and their potential impacts in a particular context.

(b) **Vulnerabilities.** These vulnerabilities are defined as the weaknesses of a given software system that may be exploited by risk sources. In this framework, vulnerabilities can be identified as disruptions to informational norms in a given context. In each context, stakeholders' privacy expectations are expressed as privacy norms. In respect to contextual integrity, norms that govern the flow of personal data from one actor to another, or others, are defined as *informa-*

tional norms. To identify possible vulnerabilities, the following steps need to be conducted.

- Identifying the relevant context on which the given software system operates.
- Identifying the key actors in the given context, i.e. data subjects, senders and recipients, and specifying their roles and responsibilities.
- Identifying the data types that are required to achieve the purposes of the given software system.
- Identifying the principles of transmission in the given context.
- Establishing the informational norms that govern the flow of personal data, whether they are implicitly or explicitly expressed.
- In each stage of the personal data lifecycle, the system's activities that may disrupt the informational norms are identified as vulnerabilities.

In summary, we adopt the contextual integrity framework to identify the appropriate flow of personal data in a given context, then use it as a baseline for identifying the software system's properties that may be exploited by risk sources.

(c) **Threats.** For each adverse event to occur, a risk source makes an action accidentally or deliberately to give rise to this event. This action is towards a given software system that processes the personal data as a valuable asset. It may happen through different threats that exploit possible vulnerabilities of that software system.

In summary, adverse events are materialised by a set of threats that exploit possible vulnerabilities of a given software system in a particular context.

(d) **Estimating the level of privacy risks.** A risk is characterised by the probability of occurrence of an adverse event and its potential impact on privacy. In so doing, the risk level is estimated in terms of severity and likelihood. Severity reflects the magnitude of a risk. Therefore, in this context, it depends on the degree of a harmful activity — e.g. identifiability and linkability — and its potential impact on data subjects. On the other hand, likelihood reflects the feasibility of a risk to occur. Therefore, it depends on the level of vulnerabilities and the capabilities of risk sources to exploit them.

In respect of risk analysis, we consider the Privacy Risk Management (PRM) [CMF+10] and the Methodology for Privacy Risk Management [Com16], which were based on the ISO 31000 Risk Management Framework [ISO09]. This step, in turn, provides the basis for risk treatment.

4. **Design strategies are a basis for architectural patterns.** Design strategies are considered as risk treatment decisions that are identified based on the analysis and assessment of the identified adverse events and their potential impacts. These strategies are intended to be objectives for achieving the privacy protection goals in a particular context. To achieve the aim of Privacy by Design, we emphasise the importance of defining preventive measures rather than protective ones. Indeed, these strategies reflect the adequate level of privacy protection as the default setting. In addition, these strategies are considered as means for mapping privacy requirement onto

software architectures. Furthermore, they are intended to illustrate appropriate conditions for selecting and applying specific architectural patterns, design patterns and their underlying Privacy-Enhancing Technologies (PETs), if any. These, in turn, help software architects to reason critically about architectural choices and their underlying patterns.

Having explained the main elements of the proposed approach, in Section 5 we introduce the ePetition system as a case study to illustrate the main steps of applying the proposed approach.

5 The ePetition System: the European Citizens' Initiative as a case study

In this section, we will introduce the European Citizens' Initiative as an instance of the ePetition system. In general, a petition can be submitted either in written or in electronic form. In this report, however, we will focus on the electronic petitions for illustration purposes.

5.1 Description

The ePetition system is an electronic information system that is used to support a formal request that is provided by organisers to a particular authority for submitting a proposal for a legal act. As an instance of petition systems, the European Citizens' Initiative [Eur12b, Eur12a], enables one million EU citizens from at least seven EU Member States to invite the European Commission to propose a legal act on issues where it has competence to legislate, such as culture, customs, transport and citizenship. For example, one of the initiatives that is currently open for collection at the time of writing is "Fair Transport Europe — equal treatment for all transport workers"[3].

Figure 1 shows the main steps of preparing and launching an initiative. The first step is setting up a citizens' committee of at least seven EU citizens. All of the committee's members need to be permanent residents or citizens of the EU Member States and old enough to vote in elections to the European Parliament. This committee acts in its capacity as the official organiser of the initiative and is responsible for preparing and managing the initiative. Secondly, the organisers need to prepare an initiative and register it in the European Commission. In order to register an initiative, the organisers need to specify the title of the initiative, the subject matter, its objectives, the committee members' personal data, and provide an email address and telephone number for the representative and their substitute. At the same time, organisers need to find a hosting provider when signatures are intended to be collected electronically by an online collection system. There are two ways of doing so: using an instance of the open source software that is provided by the European Commission and hosting it at its site; or developing their own collection system that is

[3]European Commission: European Citizens' Initiative. Retrieved from: http://ec.europa.eu/citizens-initiative/public/initiatives/open/details/2015/000002 [Accessed 8 April, 2016]

hosted in any hosting service provider. In both ways, organisers need to get a certificate from the competent national authority to verify its compliance with minimum technical requirements. Then, the certificate should be posted in the online collection system. After that, individuals, who act as signatories, are able to submit their personal data and their statements of support. To give their support for the initiative, signatories need to provide their personal data, such as full names, permanent resident, data of birth and nationality. However, in some Member States, such as France and Spain, personal identification numbers are required. Having reached the required number of signatories, organisers should send this personal data to relevant competence national authorities to verify this data and certify the number of valid statements of support. Having received all certificates from competent national authorities, organisers should submit the initiative by sending these certificates to the European Commission to take an action [Eur12b, Eur12a].

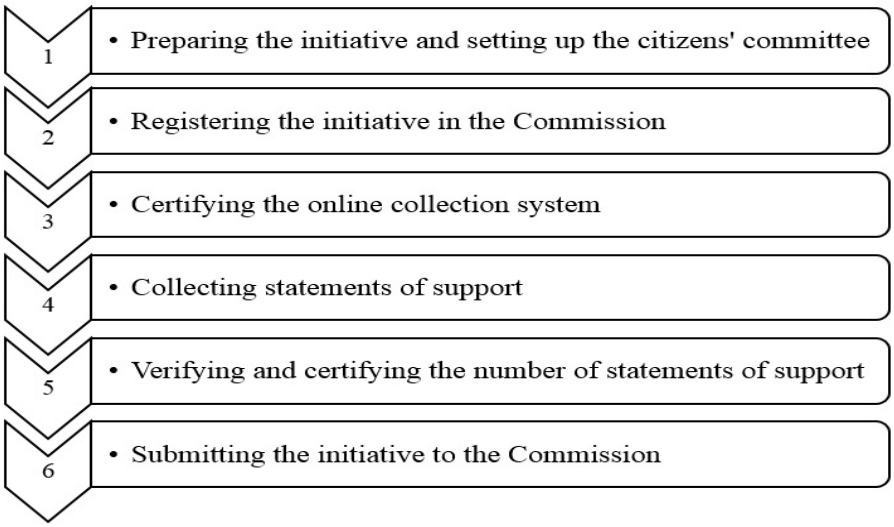

Figure 1: The main steps of organising and managing an initiative

In paper-based petitions, individuals provide their personal data, i.e. first and family names, country of permanent resident, date of birth, nationality, date and signature. Then, signatures and other personal data are manually verified by the competent national authority in each EU Member State to count the number of valid statements of support collected for that country. However, signatures are not mandatory when a statement of support is submitted electronically. Thus, an individual can only sign up once to an initiative and duplicate signatures by the same individual must be avoided [Eur11b].

In both cases, whether it is paper-based or electronic, organisers and competent national authorities act as data controllers. Thus, the organisers are required to notify the data protection authority in the EU Member State where the personal data will be processed. In addition, they are required to apply appropriate measures to protect personal data in compliance with the EU Data Protection Directive and related regulations. According to the Directive, the organisers and the competent national authorities are considered as data controllers. Therefore, referring to the Directive, personal data must be 'adequate, relevant and not excessive' in relation to the purpose of supporting the initiative and verifying the

statements of support. Accordingly, the organisers and the competent national authorities must ensure that collected personal data is not used for any purposes other than those specified for supporting the initiative and verifying the statement of support respectively. In addition, the organisers and the competent national authority must destroy all statements of support and any copies one month after submitting the initiative to the Commission or issuing the certificate respectively as specified in [Eur11b].

5.2 Functional requirements of the ePetition system

In this section, we will explain the most important functional requirements of the online collection system that is used for collecting statements of support for a given initiative. These requirements are derived from relevant legislation on the European Citizens' Initiative and technical specifications that are provided by the European Commission [Eur11a, Eur11b, Eur12b, Eur12a].

(a) The system shall detect and prevent duplicate signatures of the same signatory.

(b) The system shall provide specific administrative features for the organisers with robust multi-level access control according to the principle of least privilege.

(c) The system shall provide the organisers by the number of the statements of support for each Member State.

(d) The system shall export collected personal data in different formats.

(e) The system shall provide the initiative's registration number, title, subject matter, objectives and the contacts of the representative and their substitute.

(f) The system shall provide an electronic statement of support form through a public interface that shall be access by public without any restrictions.

(g) The system shall not allow the signatories to access their personal data once they have submitted their statements of support.

(h) The system shall prevent any unauthorised processing and protect the collected data against loss, alteration, unauthorised access or disclosure.

By analysing the referring provisions and articles of the EU Data Protection Directive, we will derive the following related privacy principles: purpose specification, collection limitation, i.e. data minimisation, use limitation, security safeguards and accountability.

6 An illustration of the proposed approach through the case study

In this section, we will illustrate the main elements of the proposed approach by analysing the functional requirements of the ePetition system as a case study, and proposing design

strategies that mitigate the most significant risks to the given system. We choose the ePetition system to initially illustrate the feasibility of the proposed approach in identifying potentially harmful activities and defining appropriate design strategies that mitigate the impact of these harms. The ePetition system has been analysed and the Privacy-Preserving ePetition System proposed in [DKD+08, GTD11]. In this report, however, we will illustrate how such solutions and design decisions can be made using design strategies based on the synthesised framework.

To assess privacy risks, adverse events need to be identified and estimated in terms of severity. For those events whose severity is high, threats that may lead to the adverse events need to be identified and their likelihood needs to be estimated. Thus, the assessed risks can be treated by applying appropriate measures to be part of design strategies. In order to do so, we start by establishing informational norms in the given context, conducting a threat analysis, analysing the significant privacy risks, and identifying appropriate treatment strategies that eliminate or mitigate the identified privacy risks.

6.1 Establishing context-relative informational norms

In this section, we will illustrate the establishment of the existing informational norms by identifying the prevailing context, actors, data attributes and transmission principles.

6.1.1 Context

The prevailing context is political participation.

6.1.2 Actors

(a) Citizens or Permanent residents of the EU Member States, who act as signatories of statements of support.

(b) Citizens' committee, which acts as a data controller, are official organisers of an initiative and responsible for its preparation and submission to the Commission.

(c) The European Commission, which acts in two capacities: registering launched initiatives and studying submitted ones; optionally, hosting online collection systems on its own servers by providing open source software.

(d) Competent national authorities at the EU Member States, which act as data controllers and legal entities for certifying online collection system, verifying related personal data, and certifying the number of valid statements of support.

(e) National data protection authority, which acts as a supervisory authority to ensure compliance with the EU Data Protection Directive and monitor its application in a Member State where personal data will be processed.

(f) Service providers, which act as data processors, are responsible for hosting online collection systems.

Member State	Paper-based	Online
France	Full first names, family names, Permanent residence: (street, number, postal code, city, country), Date of birth, Nationality, Personal identification number/ (identification document type and number), Date and Signature	Full first names, family names, Permanent residence: (street, number, postal code, city, country), Date of birth, Nationality, Personal identification number/ (identification document type and number), Date
Italy	Full first names, family names, Permanent residence: (street, number, postal code, city, country), Date and Place of birth, Nationality, Personal identification number/ (identification document type, number, issuing authority), Date and Signature	Full first names, family names, Permanent residence: (street, number, postal code, city, country), Date and Place of birth, Nationality, Personal identification number/ (identification document type, number, issuing authority), Date

Table 2: The mandatory fields of a statement of support form by France and Italy

(g) Administrators, who act as system and database administrators, are responsible for installation, configuration, operation, maintenance, security of systems hardware and software and related infrastructure.

6.1.3 Attributes

In each Member State, the mandatory fields that are required to sign up an initiative are variable according to relevant national regulations. For illustration purposes, therefore, we illustrate four scenarios that state the mandatory fields of a statement of support form by France and Italy, whether these forms are online or paper-based, in Table 2.

6.1.4 Transmission principles

Transmission principles represent the conditions under which the flows of personal data occur between the involved actors in this context. In the given context, there are seven flows of data between different parties, as shown in Figure 2.

- *Data Flow (1)*: the flow of personal data is from signatories to the organisers to support a certain initiative.
- *Data Flow (2)*: the flow of personal data is from the organisers to the service provider to retain the collected data as a data processor. In particular, these flows are abstract flows, whereas the concrete flow is from signatories to a service provider, as personal data is hosted in a service provider's infrastructure. In order to effectively analyse this

flow, however, we split it into two flows to analyse the roles and responsibilities of the data controllers and processor.

- *Data Flow (3)*: the flow of personal data is from the service provider to the organisers to process personal data in relation to their roles and responsibilities.
- *Data Flow (4)*: the flow of personal data is from the organisers to the relevant competent national authorities to verify and certify statements of support.
- *Data Flow (5)*: the flow of data is from the competent national authorities to the organisers. In particular, this flow does not involve personal data; rather it involves a certificate from each competent national authorities that only certify the number of valid statements of support.
- *Data Flow (6)*: the flow of data is from the organisers to the European Commission. In particular, this flow does not involve personal data; rather it involves certificates that only certify the number of valid statements of support.
- *Data Flow (7)*: the flow of data is from the organisers to the National Data Protection Authority where personal data will be processed. In particular, this flow does not involve personal data; rather it involves notification that illustrates types of personal data and specified purposes.

By analysing these flows, we derive a set of transmission principles that determine their occurrence in this context. These principles are in line with the privacy principles in the EU Data Protection Directive, as mentioned in Section 5.2. The first transmission principle is 'notice and consent', which means that the personal data must be collected and used with the knowledge and consent of the data subject. The second transmission principle is 'proportionality', which means the transmitted personal data must be 'adequate, relevant and not excessive' in relation to the specified purpose, and shall be protected in terms of confidentiality and integrity. The third transmission principle is confidentiality, which means the party that receives personal data is not allowed to disclose this data to other parties. These principles are considered as conditions under which "data flows 1, 2, 3 and 4" only occur, as "data flows 5, 6 and 7" do not involve personal data.

Having illustrated the main parameters that determine the appropriateness of the flows of personal data, we will analyse these flows in reference to the context-relative informational norms, as a baseline, to identify system activities that may disrupt these norms as vulnerabilities. Then, we will identify possible privacy threats that may exploit these vulnerabilities and lead to privacy harms in each stage of the personal data lifecycle.

6.2 Privacy threat analysis

Even though informational norms that govern the flow of personal data are entrenched in this context, using electronic petitions as a replacement for written petitions involve various activities that may disrupt these norms and lead to privacy violations. This means that there are many more privacy threats associated with electronic petitions than with paper-based petitions. Such threats may result from vulnerabilities of the online collection

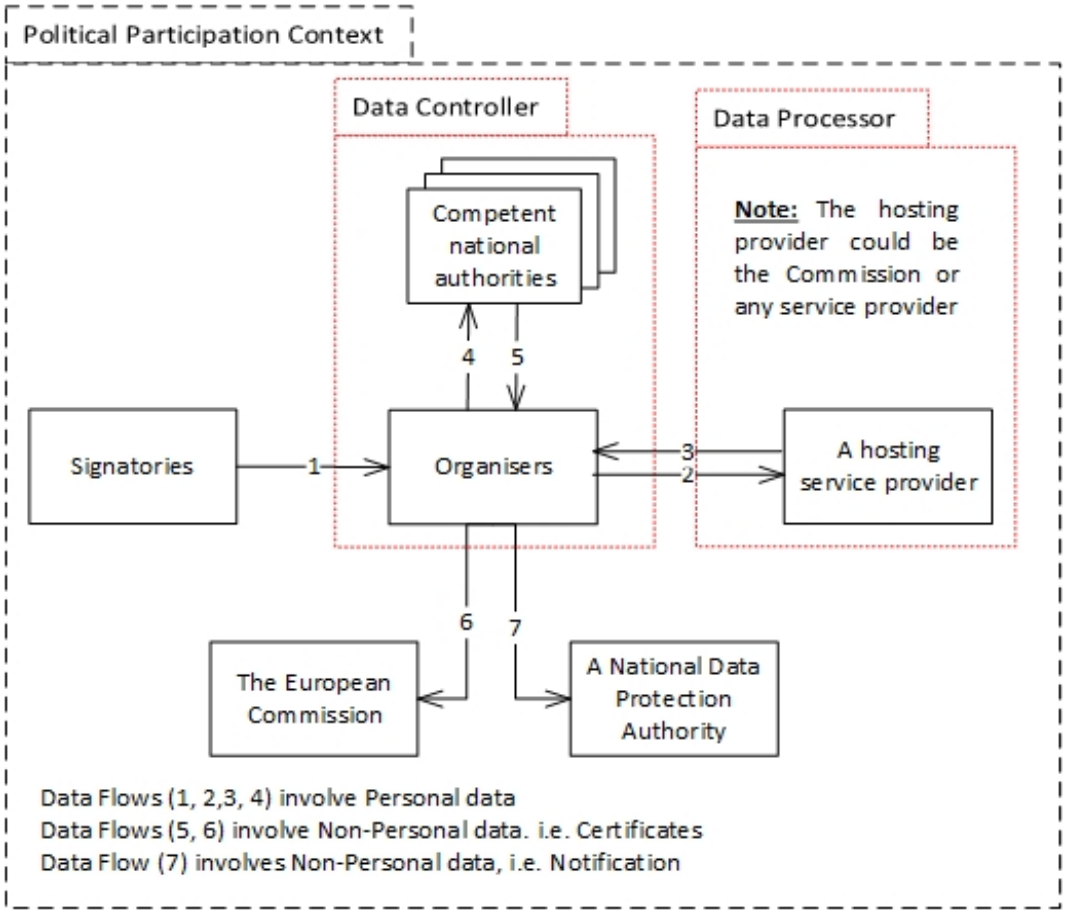

Figure 2: The main flow of personal data in the context of the political participation

system, or inappropriate security practices or measures. In this section, we will proactively identify system activities that disrupt the informational norms and lead to privacy harms to achieve the Privacy by Design foundational principle "Proactive not Reactive; Preventive not Remedial".

In order to identify system activities that lead to privacy harms in a comprehensive and concrete manner, the personal data lifecycle with reference to the taxonomy of privacy harms will be used as a basis for the contextual analysis, as shown in Figure 3. For each stage, therefore, we will analyse relevant flows of personal data in relation to the informational norms to be used as a baseline for privacy risk analysis. Then, we will identify potentially harmful activities that disrupt these norms by exploiting the vulnerabilities of the online collection system, whether accidentally or deliberately.

6.2.1 In the collection stage

(a) **Data flow:** The abstract flow of personal data (as attributes) is from signatories (as data subjects) to organisers (as a data controller) for supporting a given initiative according to the regulation on citizens' initiative (as transmission principles). However, the concrete flow of personal data is from signatories (as data subjects/senders) to

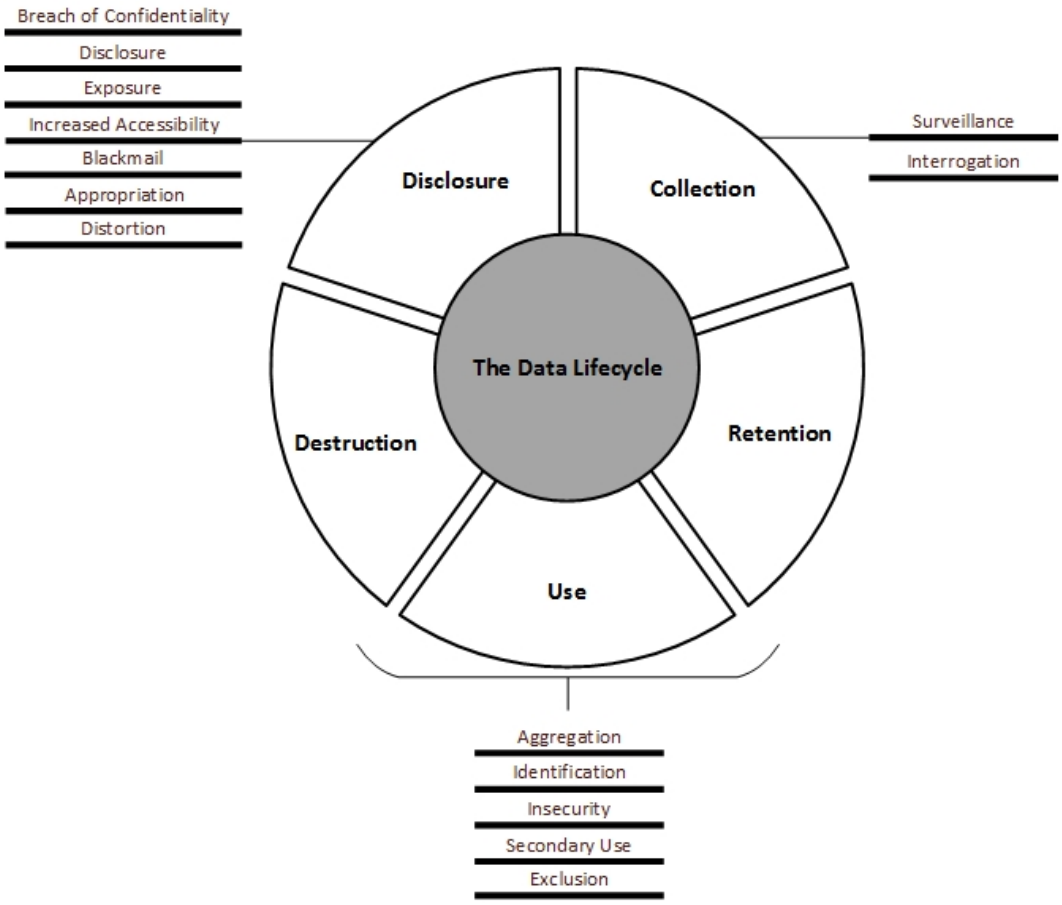

Figure 3: Privacy harms in relation to the typical stages of the personal data lifecycle

the hosting service provider (as recipients), which acts as a data processor on behalf of the organisers and under their instructions.

(b) **Informational norms:** In the context of political participation, signatories who give their support to an initiative shall provide the required personal data (Section 6.1.3) to the organisers, who are responsible for managing the initiative and collecting the minimum number of statements. The transmitted personal data in this flow shall be with the knowledge and consent of the signatories and be adequate, relevant and not excessive in relation to the specified purpose of the given initiative, and shall be protected in terms of confidentiality and integrity.

(c) **Contextual integrity:** By considering the data flows and interactions between those actors in the context of political participation, the online collection system disrupts the entrenched informational norms in terms of increasing the number of the recipients. In essence, the collected data is transferred to, processed by, and retained in, a data processor's infrastructure. This implies that system and database administrators, who work for the hosting service provider, have an access to signatories' personal data to accomplish their roles and responsibilities.

In paper-based petitions, signatories' identities and their signatures are verified manually by the organisers before providing their personal data and signing the initiative. Likewise, in the electronic petitions, the verification process of signatories' identities and their signatures' authenticity needs to be carefully considered to respect the informational norms.[4]

(d) **Harmful activities that disrupt the informational norms:** In the collection stage, privacy harms are associated with data collection methods, which may involve harmful activities that lead to adverse privacy events, such as interrogation. In more detail, interrogation as an event can be materialised by requiring signatories to provide unnecessary data as a condition of supporting a certain initiative, although the functionality of the online collection system can be achieved without this data and there is no a legal requirements to provide such data. This adverse event may happen through *collecting excessive data* as a threat that may exploit *the statement of support form* that contains irrelevant mandatory fields as a vulnerability of the online collection system. In particular, this vulnerability may be exploited by the organisers to collect inadequate, irrelevant and excessive data for purposes other than verifying and certifying the valid number of statements of support. Even though interrogation as a harmful activity is conducted with the knowledge of the data subject, its harm is in terms of making signatories feel uncomfortable about collecting such excessive data. In the context of political participation, such an activity disrupts the informational norms by collecting irrelevant attributes, i.e. types of personal data.

6.2.2 In the use stage

(a) **Data flow:** There are two main flows in this stage. First, the flow of personal data (as attributes) is from the service provider (as the senders) to the organisers (as the recipients) to process personal data in relation to their roles and responsibilities, according to the regulation on citizens' initiative (as transmission principles). Second, the flow of personal data (as attributes) is from the organisers (as the senders) to the relevant competent national authorities (as the recipients) for verification and certification purposes, according to the regulation on citizens' initiative (as transmission principles).

(b) **Informational norms:** In the context of political participation, the organisers, who are responsible for managing the initiative and collecting the minimum number of statements, shall export and prepare all statements of support, which include the required personal data (Section 6.1.3), and send them to the relevant competent national authorities, which are responsible for verifying and certifying the valid number of statements of support. The transmitted personal data in those flows shall not be disclosed to any other parties and be adequate, relevant and not excessive in relation

[4]The online collection system that is proposed by the Commission disrupts these norms in terms of collecting personal data before verifying signatories' identities and their signatures. This means that this disruption affects the transmission principles. Thus, personal data can be transferred to the organisers without initial verification.

to the specified purpose of the given initiative, and shall be protected in terms of confidentiality and integrity.

(c) **Contextual integrity:** By considering the interactions between those actors in the context of political participation, the flow of personal data does not disrupt the informational norms, which are explicitly expressed as formal and enforced regulations.

(d) **Harmful activities that disrupt the informational norms:** In the use stage, privacy harms are associated with the use of personal data, which may involve harmful activities that lead to adverse privacy events, such as insecurity and secondary use.

In more detail, insecurity as an event can be materialised by applying inadequate security measures and adopting inappropriate data handling practices. This adverse event may happen through various harmful activities as threats that may exploit the vulnerabilities of the online collection system whether personal data is at rest or in motion. In this stage, we focus on activities where data is in motion, whereas activities where data is at rest will be discussed in the retention stage. In particular, there are two possible threats that can lead to privacy harms. First, an *improper access control mechanism* as a system vulnerability may be exploited by users, who already have different levels of access control, to get and abuse of *excessive privileges* that are not related to their roles and responsibilities for malicious purposes, such as altering or deleting certain statements of support. Since this kind of harmful activity is conducted without the knowledge and consent of the data subject, its harm is in terms of making signatories are uncertain about their given support. Second, *insecure communications* as a system vulnerability may be exploited by *unauthorised outsiders* to access, analyse or alter transmitted data. This kind of threat has a potential impact in respect of uncomfortable as it increases the possibility of disclosure that leads to other privacy harms.

In addition, secondary use as an event can be materialised by using the collected data for purposes other than for which it is collected without the knowledge and consent of signatories. This adverse event may happen through two possible harmful activities as threats that may exploit the vulnerabilities of the online collection system. First, *lack of logs and audit trails* as a system vulnerability may be exploited by authorised users, i.e. organisers, national authorities, or hosting service providers, who already have legitimate privileges to deliberately *abuse* the collected data for unfair or malicious purposes, such as discrimination or identity theft. Second, *unrestricted data flow* as a system vulnerability may be exploited by users, who already have legitimate privileges, to deliberately or accidentally *misuse* the collected data for other purposes, such as commercial purposes. All these harmful activities increase the possibility of disclosure and intrusion that lead to other privacy harms.

In the context of political participation, insecurity and secondary use as harmful activities disrupt the informational norms by affecting the appropriateness of data flows in terms of involving new actors and breaching the transmission principles.

6.2.3 In the disclosure stage

(a) **Data flow:** The flow of data is from the organisers (as the senders) to the European Commission (as the recipients) for examining the initiative and adopting a formal response, according to the regulation on citizens' initiative (as transmission principles). However, this flow does not involve personal data, only certificates that certify the valid number of statements of support in each Member State.

(b) **Informational norms:** In the context of political participation, the organisers, who are responsible for managing the initiative and collecting the minimum number of statements, shall send all the certificates that have been issued by the competent national authorities to the European Commission. These certificates do not involve personal data, only the valid number of statements of support in each Member State. The transmitted data in this flow shall be relevant to the specified purpose of the given initiative, and shall be protected in terms of confidentiality and integrity.

(c) **Contextual integrity:** By considering the interactions between those actors in the context of political participation, the flow of required data does not disrupt the informational norms, which are explicitly expressed as formal and enforced regulations.

(d) **Harmful activities that disrupt the informational norms:** In respect of electronic petitions, there is no actual disclosure of personal data to other parties. However, unauthorised disclosures may happen as a result of harmful activities in other stages of personal data lifecycle as explained in each stage independently.

6.2.4 In the retention stage

(a) **Data flow:** There is no actual flow of personal data in the retention stage. However, collected personal data (as attributes) is actually retained based on the abstract flow, which is from signatories (as data subjects/senders) to organisers (as recipients), who act as a data controller, for supporting a given initiative according to the regulation on citizens' initiative (as transmission principles). In essence, the concrete flow of personal data is from signatories (as data subjects/senders) to the hosting service provider (as recipients), which acts as a data processor on behalf of organisers.

(b) **Informational norms:** In the context of political participation, signatories who give their support to an initiative shall provide the required personal data to the organisers (as the data controller), where this data is actually retained for a specific period of time by a service provider (as the data processor) on behalf of the organisers. The retained personal data shall be protected against unauthorised access, use, modification, disclosure and destruction.

(c) **Contextual integrity:** By considering the interactions between those actors in the context of political participation, the online collection system disrupts the entrenched informational norms in terms of increasing the number of the recipients. In particular, collected personal data is not retained physically in the data controller's premises.

This means that system and database administrators who work for the hosting service provider have access to signatories' personal data to accomplish their roles and responsibilities.

(d) **Harmful activities that disrupt the informational norms:** In the retention stage, privacy harms are associated with the storage of personal data, which may involve harmful activities that lead to adverse privacy events, such as insecurity, secondary use, aggregation and exclusion.

In more detail, insecurity as an event can be materialised by applying inadequate security measures and adopting inappropriate data handling practices. This adverse event may happen through various harmful activities as threats that may exploit the vulnerabilities of the online collection system whether the collected data is at rest or in motion. In this stage, we focus on activities where the data is at rest. In particular, there are five possible threats that can lead to privacy harms. First, *improper access control mechanism* as a system vulnerability may be exploited by the database administrator and users, who already have different levels of access control, to get and abuse *excessive privileges* that are not related to their roles and responsibilities for malicious purposes, such as accessing, altering or deleting certain attributes or a whole statement of support. Second, *improper security configurations* as a system vulnerability may be exploited by *unauthorised* outsiders to access, alter or delete retained data. Such an activity increases the possibility of disclosure that leads to other privacy harms. Third, *inappropriate retention schedule* as a system vulnerability may be exploited by system and database administrators to accidentally use and keep data during the *unlawful retention* period. Fourth, *improper authentication mechanisms* as a system vulnerability may be exploited by unauthorised outsiders to *impersonate* signatories and get access to their retained personal data for malicious purposes. Fifth, *insecure communications* as a system vulnerability may be exploited by *unauthorised* outsiders to access signatories' transmitted data through traffic analysis. As this kind of threat is conducted without the knowledge of the data subject, its harm is in terms of making signatories are uncertain about their given support.

In addition, secondary use as an event can be materialised by using the collected data for purposes other than for which it is collected without the knowledge and consent of signatories. This adverse event may happen through two possible harmful activities as threats that exploit the vulnerabilities of the online collection system. First, *lack of logs and audit trails* as a system vulnerability may be exploited by authorised users, i.e. the database administrator and users, who already have legitimate privileges, to deliberately *abuse* the collected data for unfair and malicious purposes, such as discrimination or identity theft. Second, *unrestricted data retrieval* as a system vulnerability may be exploited by the database administrator and users, who already have legitimate privileges, to deliberately or accidentally *misuse* the collected data for other purposes, such as commercial purposes. All these harmful activities increase the possibility of disclosure and intrusion that lead to other privacy harms.

In addition, aggregation as an event can be materialised by performing activities that combine retained data with other pieces of data from different contexts or from the

same contexts in different times. This adverse event may happen by authorised users through *data integration* as a threat that may exploit *retaining identifiable personal data* as a system vulnerability. As a result, this aggregated data is not expected by signatories when they provide the required data for supporting the given initiative. Indeed, aggregation as a harmful activity leads to privacy harms, such as dignitary harms as it disrupts signatories' expectations in an unanticipated manner. In addition, it facilitates creating sophisticated profiles for signatories. Those profiles that have details about all supported initiatives may be used in the future for judgement or important decisions. However, profiles may be incomplete or have misleading data, which, in turn, leads to distortion as an adverse event. Additionally, profiles may be exploited for other purposes that may lead to adverse events, such as intrusion, which disrupts signatories' private affairs and may make them feel uncomfortable and uneasy.

Furthermore, exclusion as an event can be materialised by denying signatories' access requests for exercising their access rights. This adverse event may happen through *denial of access* as a threat that may exploit *lack of subject access mechanisms* as a system vulnerability. Such an event may make signatories feel vulnerable and uncertain about their personal data. In principle, signatories as data subjects have the right to access their personal data until the initiative is submitted to the European Commission. This is to ensure that their personal data is not modified, altered or lost, as well as to ensure their statements of support are counted. In order to implement such mechanisms, a robust authentication mechanism is required to verify signatories' identities and their credentials before getting access to relevant personal data.

Insecurity, secondary use and aggregation, as harmful activities, are conducted without the knowledge and consent of the data subject. Such activities disrupt the informational norms by involving new actors and breaching the transmission principles.

6.2.5 In the destruction stage

(a) **Data flow:** The flow of personal data (as attributes) is from the hosting service provider (as the senders) to the competent destruction actors (as the recipients), whether those actors are internal business units or third parties that provide secure destruction services. The flow is for destruction purposes according to the destruction process that has been agreed by the organisers in their role of data controller.

(b) **Informational norms:** In the context of political participation, the hosting service provider (as the data processor) shall send all copies of the personal data to competent destruction actors according the data controller's instructions at the end of the specified period of time for retention. The transmitted personal data in this flow shall be protected against unauthorised access, use, modification and disclosure, and shall be securely destroyed in a manner that cannot be recovered.

(c) **Contextual integrity:** By considering the interactions between those actors in the context of political participation, the online collection system disrupts the entrenched informational norms in terms of increasing the number of the recipients, i.e. data

processor and other third parties, if any. In particular, collected personal data is not retained physically in the data controller's premises. Therefore, having fulfilled the specified purpose and ending legal retention time, system and database administrators who work for the hosting service provider have a responsibility to destroy all copies of retained data as part of their roles and responsibilities.

(d) **Harmful activities that disrupt the informational norms:** In the destruction stage, privacy harms are associated with the disposal of personal data, which may involve harmful activities that lead to adverse privacy events, such as insecurity and secondary use.

In more detail, insecurity as an event can be materialised by applying inadequate security measures and adopting inappropriate data handling practices. This adverse event may happen through various harmful activities as threats that may exploit the vulnerabilities of the online collection system. In particular, there are three threats that can lead to privacy harms. First, *improper data backup documentation* as a vulnerability that may be exploited by the database administrator through keeping copies of *undestroyed backups* of personal data. Second, *insecure destruction process* as a system vulnerability that may be exploited by the database administrator and competent destruction units through performing an *unauthorised destruction*. Third, *insufficient destruction methods* as a system vulnerability that may be exploited by competent destruction units through performing *data recovery* from destroyed media. All these harmful activities increase the possibility of disclosure and intrusion that lead to other privacy harms.

In addition, secondary use as an event can be materialised by using the retained data for purposes other than for which it is collected without the knowledge and consent of signatories. This adverse event may happen through the *misuse* of the retained data as a threat posed by authorised users, who work for the hosting service provider or competent destruction units. The threat may happen as a result of successful exploitation of *insecure destruction process* as a system vulnerability whether accidentally or deliberately for illegitimate purposes. This, in turn, increases the possibility of disclosure as an adverse event, which has privacy harms, such as affecting signatories in terms of supporting certain initiatives that are related to sensitive issues.

Insecurity and secondary use, as harmful activities, are conducted without the knowledge and consent of the data subject. Such activities disrupt the informational norms by involving new actors and breaching the transmission principles.

6.3 Risk analysis

Having identified vulnerabilities, threats and adverse events, we now conduct a privacy risk analysis and assessment. For each adverse event, we will illustrate all related threats and corresponding vulnerabilities. In addition, we will estimate its severity based on the degree of the harmful activities and its impact. Likewise, the likelihood is estimated based on the feasibility of a risk to occur, i.e. the capability of the risk sources and the level of vulnerabilities of the online collection system, as shown in Table 3.

No.	Vulnerability	Threat	A.E	SE.	LI.	R.
	Data Collection Stage:					
RIS01	Irrelevant mandatory fields	Excessive data	Interrogation	M	L	S
	Data Use Stage:					
RIS02	Improper access control	Excessive privileges	Insecurity	S	L	L
RIS03	Insecure communications	Unauthorised access	Insecurity	M	L	S
RIS04	Unrestricted data flow	Misuse	Secondary use	M	M	M
RIS05	Lack of logs and audit trails	Privileges abuse	Secondary use	M	L	S
	Data Disclosure Stage:					
	-	-	-	-	-	-
	Data Retention Stage:					
RIS06	Improper access control	Excessive privileges	Insecurity	S	L	L
RIS07	Improper security configurations	Unauthorised access	Insecurity	M	L	S
RIS08	Improper authentication mechanisms	Impersonation	Insecurity	M	L	S
RIS09	Insecure communications	Unauthorised access	Insecurity	M	N	L
RIS10	Identifiable personal data	Data integration	Aggregation	M	M	M
RIS11	Lack of subject access mechanisms	Denial of access	Exclusion	S	L	L
RIS12	Unrestricted data retrieval	Misuse	Secondary use	M	M	M
RIS13	Lack of logs and audit trails	Privileges abuse	Secondary use	M	L	S
RIS14	Inappropriate retention schedule	Unlawful retention	Insecurity	M	S	M
	Data Destruction Stage:					
RIS15	Improper backup documentation	Undestroyed backups	Insecurity	M	S	M
RIS16	Insecure destruction process	Unauthorised destruction	Insecurity	M	L	S
RIS17	Insufficient destruction methods	Data recovery	Insecurity	S	L	L
RIS18	Insecure destruction process	Misuse	Secondary use	M	L	S

A.E: Adverse event, **SE:** Severity, **LI:** Likelihood, **R:** Risk, **M:** Maximum, **S:** Significant, **L:** Limited, **N:** Negligeable

Table 3: The significant privacy risks

Having conducted a privacy risk analysis and estimated the likelihood and severity of each adverse event, we now emphasise the most significant risks that have high potential impacts on signatories' privacy: insecurity, secondary use and aggregation.

6.4 Requirements Elicitation

Having identified harmful activities that can lead to privacy harms in each stage of the personal lifecycle in a comprehensive and concrete manner, in this section we will elicit explicit privacy requirements that need to be satisfied to mitigate privacy concerns and ensure compliance with legal and regulatory requirements, as show in Table 4.

Data Collection Stage:

REQ01: The system shall provide a clear and understandable privacy notice to signatories before collecting their personal data.

REQ02: The system shall restrict the collection of personal data to be adequate, relevant, and not excessive by implementing the specified statement of support forms as well as with the knowledge and consent of signatories.

Data Use Stage:

REQ03: The system shall implement a robust authentication mechanism to verify the identity of system administrators and users, and prevent unauthorised access to retained personal data.

REQ04: The system shall implement a robust access control model in relation to the assigned roles and responsibilities of the system administrator and users, as well as restrictive policies.

REQ05: The system shall encrypt transmitted personal data over networks to prevent unauthorised access.

REQ06: The system shall restrict the use of personal data to processes that achieve the purpose of verifying and certifying statements of support, for which signatories have provided their explicit consent.

REQ07: The system shall maintain all the system administrators' and users' activities for audit and monitoring purposes.

Data Disclosure Stage:

REQ08: The system shall not disclose personal data to third parties without consent of signatories.

Data Retention Stage:

REQ09: The system shall implement a robust authentication mechanism to verify the identity of the database administrator and users, and prevent unauthorised access to retained personal data.

REQ10: The system shall implement a robust access control model in relation to the assigned roles and responsibilities of the database administrator and users, as well as restrictive policies.

REQ11: The system shall encrypt the primary and backup copies of retained personal data to prevent unauthorised access.

REQ12: The system shall prevent the system and database administrator and users from altering or deleting retained personal data without the knowledge of signatories before it has been verified and certified by the competent national authorities.

REQ13: The system shall implement a robust authentication mechanism to verify the identity of signatories and prevent unauthorised access to retained personal data.

REQ14: The system shall encrypt transmitted personal data over public networks to prevent unauthorised access.

REQ15: The system shall implement the principle of separation of duties to prevent users and the database administrator from retrieving all or large amounts of personal data. **REQ16:** The system shall provide signatories with access to their personal data for review and update before sending statements of support to the competent national authorities. **REQ17:** The system shall restrict the access and retrieval of personal data by the database administrator and users to approved requests only. **REQ18:** The system shall maintain all the database administrators' and users' activities for audit and monitoring purposes. **REQ19:** The system shall retain personal data only for the period that is required by regulations.
Data Destruction Stage:
REQ20: The system shall not allow users to access and use retained personal data by the end of the specified retention period. **REQ21:** The system shall not allow users to access and use backups copies by the end of the specified retention period. **REQ22:** The system shall provide automatic notifications to alarm the system and database administrators by the end of the specified retention schedule to dispose of retained personal data in a sufficient manner that prevents loss, misuse, or unauthorised access or destruction.

Table 4: Privacy requirements in each stage of the personal data lifecycle

In summary, the case study initially illustrates how various harmful activities in each stage of the personal data lifecycle yield a set of privacy harms that have potential impact on data subjects' privacy. Thus, the concrete privacy requirements are elicited based on the result of the privacy risk analysis and assessment. This, in turn, provides a traceable manner for tracking each attribute of personal data through the entire lifecycle to ensure its compliance with specified purposes. This initially illustrates that the proposed approach will support software engineers in identifying and assessing privacy harms in a comprehensive and concrete manner. This approach, therefore, in some way confronts the challenges of relying on engineers expertise in translating the foundational principles of Privacy by Design into system requirements.

6.5 Design Specification

In the preceding subsections, we illustrated the synthesised privacy threat analysis framework as an element of the proposed approach. As a result of this illustration, we conducted privacy impact assessment and elicited concrete privacy requirements for the electronic petition system. In this section, we will illustrate design strategies as the fourth element of the proposed approach. In this context, design strategies are considered as objectives for achieving privacy protection goals. These strategies aim to address privacy concerns and support

mapping privacy requirements onto software architectures. In particular, these strategies are intended to be highly abstracted methods for achieving or at least supporting privacy protection goals by specifying treatment options that lead to appropriate architectural patterns, design patterns and underlying Privacy-Enhancing Technologies (PETs) if any. For each design strategy, we will identify the main conditions of application, such as purpose, privacy concerns, privacy requirements, treatment options, privacy protection goals, privacy principles and potential consequences.

In this report, we are not going to propose a novel solution; rather, we attempt to explain how to illustrate design strategies using existing solutions from the privacy literature. In respect to the case study, there are two different choices that lead to various architectural decisions that fulfil the elicited privacy requirements. Indeed, the decision of choosing the appropriate solution is a strategic decision that can be made by the high management with stakeholders' participation. The first choice is an anonymous ePetition system, which can be achieved by selecting the data minimisation strategy. The second choice is a compliant ePetition system with the relevant regulations, which can be achieved by selecting the data adequacy, data subject participation, and policy enforcement strategies. These strategies will be further explained in the following sections.

6.5.1 Strategy 1: Data minimisation

- **Aim:** this strategy aims to provide appropriate authentication mechanisms as well as personal data verification before supporting a certain initiative. This can be achieved by verifying the identity of the signatories by the competent national authorities and ensuring that they are old enough to vote in European Parliament elections as required by regulations, then issuing anonymous credentials to be used for supporting a certain initiative. In addition, this strategy provides a way to detect and prevent issuing duplicate certificates for the same individual.

- **Targeted privacy concerns:** this strategy addresses *interrogation*, *insecurity*, *secondary use*, *aggregation*, *disclosure* and *exclusion* as harmful activities that lead to privacy harms.

- **Related vulnerabilities:** this strategy addresses the following vulnerabilities: *irrelevant mandatory fields* and *retaining identifiable personal data*.

- **Related privacy risks:** RIS01, RIS10

- **Related privacy requirements:** REQ01, REQ02

  In addition, this strategy addresses security related requirements that enforce these decisions: REQ03, REQ04, REQ05, REQ07, REQ08, REQ09, REQ10, REQ12, REQ13, REQ14, REQ15, REQ17, REQ18

- **Related privacy protection goals:** this strategy supports unlinkability, intervenability and transparency as privacy protection goals.

- **Related privacy principles:** the supported protection goals achieve the following privacy principles: openness, purposes, consent, collection limitation, use, retention, disclosure limitation, accuracy, and security.

- **Treatment options:** the related risks are with a significant severity and a limited likelihood; therefore, they will be avoided by implementing preventive security measures that reduce their severity and likelihood.

- **Constraints:** the regulation that governs the European Citizens' Initiative specifies the required personal data for verification and certification purposes; therefore, this strategy is subject to legal constraints. In addition, there is another design constraint, which requires electronic identification cards to be used for interactive verification and digital signature to issue anonymous credentials that can be used by the online collection system as an authentication mechanism.

- **Consequences:** applying such a strategy requires more consideration of accountability in terms of dealing with claims that abusing unlinkability. In particular, this strategy is based on 'avoidance' as a treatment strategy to entirely avoid collecting and retaining personal data. This means that the functionality of the electronic petition system is reconsidered by using anonymous credentials instead of identifiable personal data. This, in turn, entails that only anonymous credentials and transactions details are retained in the ePetition system's database.

  In addition, applying such a strategy requires more consideration of implementing strong security measures to provide an adequate level of privacy protection. In particular, robust authentication and authorisation mechanisms shall be implemented to avoid unauthorised access during the interactive verification.

6.5.2 Strategy 2: Data adequacy

- **Aim:** this strategy aims to apply the principle of data minimisation by collecting only adequate, relevant and not excessive data in relation to the specified purpose, in this case, verification and certification purpose.

- **Targeted privacy concerns:** this strategy addresses *interrogation* as a harmful activity that leads to privacy harms.

- **Related vulnerabilities:** this strategy addresses *irrelevant mandatory fields* as a system vulnerability that may be exploited by *excessive data* as a possible threat.

- **Related privacy risks:** RIS01

- **Related privacy requirements:** REQ02

  In addition, this strategy addresses security related requirements that enforce these decisions: REQ13 and REQ14

- **Related privacy protection goals:** this strategy supports intervenability and transparency as privacy protection goals.

- **Related privacy principles:** the supported protection goals achieve the following privacy principles: collection limitation, i.e. data minimisation, and purpose.
- **Treatment options:** the related risk is with a significant severity and a limited likelihood; therefore, it will be avoided by implementing preventive security measures that reduce its severity and likelihood. In order to achieve that, the online statement of support form shall only contain the mandatory fields in relation to the specified purpose.
- **Constraints:** the regulation that governs the European Citizens' Initiative specifies the required personal data for verification and certification purposes; therefore, this strategy is subject to legal constraints.
- **Consequences:** applying this strategy requires more consideration of implementing strong security measures to provide an adequate level of privacy protection. In particular, robust authentication mechanisms and security protocols, which establish secure connections for protecting transmitted personal data, shall be implemented.

6.5.3 Strategy 3: Data subject participation

- **Aim:** this strategy aims to implement the data subjects' rights by providing appropriate privacy notice and subject access mechanisms to exercise control over their personal data and be able to review, amend or delete that data where it is inaccurate.
- **Targeted privacy concerns:** this strategy addresses the *exclusion* as a harmful activity that leads to privacy harms.
- **Related vulnerabilities:** this strategy addresses the *lack of subject access mechanisms* as a system vulnerability that may be exploited by *denial of access* as a possible threat.
- **Related privacy risks:** RIS11
- **Related privacy requirements:** REQ16

  In addition, this strategy addresses security related requirements that enforce these decisions: REQ13
- **Related privacy protection goals:** this strategy supports intervenability and transparency as privacy protection goals.
- **Related privacy principles:** the supported protection goals, in turn, achieve the following privacy principles: openness, consent, access, accuracy and compliance.
- **Treatment options:** the related risk is with a limited severity and likelihood; therefore, it will be reduced by implementing preventive security measures that reduce its severity and likelihood. In order to achieve that, appropriate privacy notice and subject access mechanisms will be implemented to exercise control over personal data.

– **Constraints:** the regulation that governs the European Citizens' Initiative specifies the required personal data for verification and certification purposes; therefore, this strategy is subject to legal constraints. This implies another constraint that may affect the purpose of collecting and using personal data, such as statements of support shall not be amended or deleted after having been sent to the competent national authorities.

– **Consequences:** applying this strategy may produce other privacy risks; therefore, it requires more consideration of applying strong security measures to provide an adequate level of privacy protection. As the retained data is identifiable personal data, a robust authentication mechanism shall be implemented to avoid unauthorised access or signatories impersonation.

6.5.4 Strategy 4: Policy enforcement

– **Aim:** this strategy aims to enforce and restrict the uses of personal data to the privacy policy by implementing compliance mechanisms. This aim can be achieved by implementing appropriate role-based access control in relation to users' and administrators' roles and responsibilities. In addition, this strategy includes maintaining logs and audit trails for compliance purposes. Thus, each attribute can be traced in all the stages of the personal data lifecycle to ensure that is restricted to specified purpose.

– **Targeted privacy concerns:** this strategy addresses the *insecurity*, *aggregation* and *secondary use* as harmful activities that lead to privacy harms.

– **Related vulnerabilities:** this strategy addresses the *unrestricted data retrieval*, *lack of logs and audit trails*, *retained identifiable personal data*, and *inappropriate retention schedule* as system vulnerabilities that may be exploited by *misuse*, *privileges abuse*, *data integration* and *unlawful retention* as possible threats.

– **Related privacy risks:** RIS02, RIS03, RIS04, RIS05, RIS06, RIS07, RIS10, RIS11, RIS12, RIS13, RIS14

– **Related privacy requirements:** REQ01, REQ06, REQ07, REQ08, REQ12, REQ15, REQ17, REQ18, REQ19, REQ20, REQ21, REQ22

  In addition, this strategy addresses security related requirements that enforce these decisions: REQ03, REQ04, REQ05, REQ09, REQ10, REQ11

– **Related privacy protection goals:** this strategy supports confidentiality and integrity as security properties, which, in turn, support privacy protection goals.

– **Related privacy principles:** the supported protection goals, in turn, achieve the following privacy principles: use, retention and disclosure limitation, security, and compliance.

– **Treatment options:** the related risks are with a significant severity but a likelihood that ranges from negligible to limited; therefore, they will be reduced by implementing

preventive security measures that reduce their severity. In order to achieve that, compliance and monitoring mechanisms will be implemented to restrict the uses of personal data to the privacy policy.

- **Constraints:** the regulation that governs the European Citizens' Initiative specifies the required personal data for verification and certification purposes; therefore, this strategy is subject to legal constraints. This implies the roles and responsibilities of the data controllers and processor need to be clearly specified in the privacy policy to be enforced and audited.

- **Consequences:** applying this strategy requires more consideration of implementing strong security measures to provide an adequate level of privacy protection. In particular, proper security configurations, robust authentication and authorisation mechanisms shall be implemented in relation to the assigned roles and responsibilities to avoid unauthorised access. Furthermore, data encryption and security protocols, which establish secure connections for protecting transmitted personal data, shall be implemented to prevent unauthorised access and disclosure.

In summary, design strategies are identified as objectives to achieve privacy protection goals. In particular, each design strategy addresses one or more potential privacy harms that may happen as a result of various harmful activities. Such activities may exploit the vulnerabilities of the online collection system whether accidentally or deliberately. Based on the materialised privacy risks, each strategy has a treatment option in relation to the likelihood of successful exploitation and the impact of the privacy harm. These options vary in the ways they respond to the privacy risk whether avoidance, reduction, transfer or acceptance. In addition, each design strategy may have some consequences that may affect other design strategies or other quality attributes, such as accountability. Furthermore, design strategies may have some constraints whether design or legal constraints, which, in turn, affect design decisions. Indeed, these strategies are design decisions to achieve an adequate level of privacy protection. However, enforcing these decisions requires implementing appropriate security measures, such as encryption, robust authentication and authorisation mechanisms. Thus, each design strategy addresses security requirements that enforce related design decisions. In so doing, design strategies can be used as criteria for applying appropriate privacy patterns and their underlying Privacy-Enhancing Technologies (PETs), if any.

Therefore, design strategies are intended to support the interaction between privacy requirements and software architectures. This interaction facilitates mapping these requirements onto architectural patterns to refine, define, analyse and evaluate the software architecture. In essence, identifying such strategies supports selecting appropriate architectural choices in a rational manner in the early stages of the design process. This means that architectural choices that encompass these strategies can be used as inputs for a systematic cost-benefit analysis method for analysing, evaluating and selecting alternative architectural decisions.

7 Conclusion and future work

Privacy, as a fundamental right, is a multidimensional concept that has legal, social and political aspects. This implies that these various perceptions of privacy are influenced by political, social and economic changes, as well as by information technology advancements. Accordingly, privacy definitions and principles are typically given at a high level of abstraction. In response, Privacy by Design has emerged as a proactive approach for embedding privacy requirements into the early stages of the design of information technologies. However, its foundational principles are given at a high level of abstraction without accompanying methodologies and guidelines for its integration into the software development process.

Engineering Privacy by Design involves several challenges, which include a lack of holistic, systematic and integrative methodologies that address the complexity and variability of privacy, and support the translation of its foundational principles onto operational requirements that can be reconciled with technical requirements.

To address these challenges, we derived a set of criteria that need to be considered when devising such methodologies and guidelines. First, an appropriate interpretation of privacy needs to be understood by software engineers. Instead of referring to abstract definitions, a bottom-up contextualised approach can be used to understand activities that lead to privacy harms in each particular context. To meet this complexity, the taxonomy of privacy can be adopted to understand privacy violations, which involve a variety of harmful activities. By adopting such a taxonomy, software engineers can focus on software system activities that may have privacy impacts rather than referring to abstract definitions and principles. Second, reasonable privacy expectations and concerns need to be understood and considered by software engineers. In some ways it is understandable that these expectations vary; to meet this variability, the contextual integrity framework can be adopted to understand privacy expectations and their implications in each context. Third, potentially harmful activities that lead to privacy harms need to be identified in a concrete and meaningful manner. To meet this challenge, a privacy threat analysis framework can be developed by synthesising the taxonomy of privacy and the contextual integrity framework. Fourth, full protection of personal data needs to be ensured from collection to destruction. To meet this challenge, the personal data lifecycle can be used as a basis for analysis to ensure that privacy concerns in each stage are appropriately identified and addressed. This, in turn, supports the traceability of privacy requirements and provides a common language among stakeholders, as privacy legislation and principles are given in relation to the typical stages of personal data lifecycle. Fifth, the degree to which privacy is required needs to be specified by software engineers. To meet this challenge, treatment options that address the identified privacy concerns can be determined in relation to the reasonable expectations. Thus, these options specify the adequate level of privacy protection that can be implemented as the default setting. Sixth, creative architectural choices need to be specified in a positive-sum and rational manner, as these decisions are hard to change in the later stages of the design process. To meet this challenge, design strategies that address the identified potential privacy harms at architectural levels can be identified. In particular, identifying such strategies supports the interaction between privacy requirements and software architectures. This, in turn, facilitates mapping privacy requirements onto architectural patterns for analysing, evaluating and selecting alternative architectural decisions.

To this end, we have derived a set of criteria to address the main challenges; based on these criteria, we have put forward a proposal for engineering Privacy by Design. Furthermore, we have illustrated the main elements of the proposed approach through the ePetition system as a case study. The case study initially illustrates the possibility of adopting the proposed approach and its potential role in identifying and addressing potential privacy harms that are result from software system activities in each stage of the personal data lifecycle in a concrete and meaningful manner.

The initial results of the case study help to inform our plans for future work in this area. In particular, this work can be divided into three main parts. First, we will formulate the synthesised privacy threat analysis framework to identify and address software system activities that lead to privacy harms in a contextual manner. Second, we intend to define and analyse additional case studies that have different privacy concerns in various contexts, including electronic toll pricing systems and electronic voting systems. The former has been chosen to illustrate design strategies that address privacy concerns where designing an anonymous eToll pricing system is not applicable. The latter has been chosen to illustrate design strategies that not only address voters' privacy concerns, but also candidates' privacy concerns. Third, we plan to identify useful privacy design strategies to be used as a basis for defining architectural patterns, along with their corresponding design patterns and underlying Privacy-Enhancing Technologies (PETs). These patterns will be evaluated in relation to the foundational principles of Privacy by Design and their underlying Fair Information Practice Principles (FIPPs). In so doing, this research will overcome the shortcomings of the Privacy by Design approach and help to bridge the acknowledged gap.

In conclusion, this report has laid the foundations for developing a holistic, systematic and principled methodology that addresses the complexity and variability of privacy, identifies potentially harmful activities in a concrete and meaningful manner, and supports the translation of the foundational principles of Privacy by Design into engineering activities.

References

[BBK+12] C. Bier, P. Birnstill, E. Krempel, H. Vagts, and J. Beyerer. Enhancing Privacy by Design from a Developers Perspective. In *Privacy Technologies and Policy: First Annual Privacy Forum (APF 2012)*, pages 73–85. Springer, 2012.

[Bec12] K. Beckers. Comparing privacy requirements engineering approaches. In *2012 Seventh International Conference on Availability, Reliability and Security (ARES)*, pages 574–581. IEEE, 2012.

[Can14] J. C. Cannon. *Privacy in Technology: Standards and Practices for Engineers and Security and IT Professionals*. International Association of Privacy Professionals, 2014.

[Cav06] A. Cavoukian. Creation of a Global Privacy Standard. https://www.ipc.on.ca/images/Resources/gps.pdf, 2006.

[Cav09] A. Cavoukian. Privacy by Design. https://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf, 2009.

[Cav10] A. Cavoukian. Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=953, 2010.

[Cav12] A. Cavoukian. Privacy by Design [Leading Edge]. *IEEE Technology and Society Magazine*, 31(4):18–19, 2012.

[CMF+10] A. Cavoukian, M. Monica, A. Fariba, R. Dan, and K. Jeff. Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default. https://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf, 2010.

[Com16] Commission Nationale de l´Informatique et des Libertés (CNIL). Methodology for Privacy Risk Management. https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf, 2016.

[CSC14] A. Cavoukian, S. Shapiro, and R. J. Cronk. Privacy Engineering: Proactively Embedding Privacy by Design. https://www.privacybydesign.ca/content/uploads/2014/01/pbd-priv-engineering.pdf, 2014.

[CSD+10] A. Cavoukian, J. Stoddart, A. Dix, I. Nemec, V. Peep, and M. Shroff. Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/10-10-27_Jerusalem_Resolutionon_PrivacybyDesign_EN.pdf, 2010.

[CSXM09] X. Cui, Y. Sun, S. Xiao, and H. Mei. Architecture Design for the Large-Scale Software-Intensive Systems: A Decision-Oriented Approach and the Experience. In *14th IEEE International Conference on Engineering of Complex Computer Systems*, pages 30–39. IEEE Conference Publications, 2009.

[DA06] P. Dourish and Ken A. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *HumanComputer Interaction*, 21(3):319–342, 2006.

[DFF14] M. F. Dennedy, J. Fox, and T. Finneran. *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*. Apress, 2014.

[DKD+08] C. Diaz, E. Kosta, H. Dekeyser, M. Kohlweiss, and G. Nigusse. Privacy preserving electronic petitions. *Identity in the Information Society*, 1(1):203–219, 2008.

[DWS+11] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1):3–32, 2011.

[Eur11a] European Commission. Commission Implementing Regulation No 1179/2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:301:0003:0009:EN:PDF, 2011.

[Eur11b] European Commission. Regulation (EU) No 211/2011 of the European Parliament and of the Council. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02011R0211-20131008&from=EN, 2011.

[Eur12a] European Commission. The European Citizens' Initiative. http://ec.europa.eu/citizens-initiative/public/welcome, 2012.

[Eur12b] European Commission, Secretariat-General. Guide to the European Citizens' Initiative. http://ec.europa.eu/dgs/secretariat_general/citizens_initiative/index_en.htm, 2012.

[GdA16] S. Gürses and J.M. del Alamo. Privacy Engineering: Shaping an Emerging Field of Research and Practice. *IEEE Security & Privacy*, 14(2):40–46, 2016.

[GTD11] S. Gürses, C. Troncoso, and C. Diaz. Engineering privacy by design. *Computers, Privacy & Data Protection*, 14, 2011.

[Han11] M. Hansen. Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In *Privacy and Identity Management for Life*, pages 14–31. Springer Berlin Heidelberg, 2011.

[HJR15] M. Hansen, M. Jensen, and M. Rost. Protection Goals for Privacy Engineering. In *Security and Privacy Workshops (SPW)*, pages 159–166. IEEE, 2015.

[HZNF15] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz. A Taxonomy for Privacy Enhancing Technologies. *Computers & Security*, 53:1–17, 2015.

[ISO09] ISO. ISO 31000 - Risk management – Principles and guidelines. http://www.iso.org/iso/home/standards/iso31000.htm, 2009.

[KKG07] C. Kalloniatis, E. Kavakli, and S. Gritzalis. Using privacy process patterns for incorporating privacy requirements into the system design process. In *The Second International Conference on Availability, Reliability and Security (ARES 2007)*, pages 1009–1017. IEEE Conference Publications, 2007.

[KKG08] C. Kalloniatis, E. Kavakli, and S. Gritzalis. Addressing privacy requirements in system design: the PriS method. *Requirements Engineering*, 13(3):241–255, 2008.

[KLL05] T. Kim, S. Lee, and E. Lee. Privacy engineering in ubiComp. *Computational Science And Its Applications*, 3482:1279–1288, 2005.

[NCM+15] N. Notario, A. Crespo, Y. S. Martín, J. M. Del Alamo, D. Le Métayer, T. Antignac, A. Kung, I. Kroener, and D. Wright. PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 151–158. IEEE, 2015.

[Nis09] H. F. Nissenbaum. *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.

[OGD+05] Y. Onn, M. Geva, Y. Druckman, A. Zyssman, R. Timor, I. Lev, A. Maroun, T. Maron, Y. Nachmani, Y. Simsolo, S. Sicklai, A. Fuches, M. Fishman, S. Packer, and L. Pery. Privacy in the Digital Environment. *Haifa Center of Law & Technology*, pages 1–12, 2005.

[Org13] Organisation for Economic Co-operation and Development (OECD). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, 2013.

[PH10] A. Pfitzmann and M. Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf, 2010.

[PKK01] A. Pfitzmann, M. Kohntopp, and M. Kohntopp. Anonymity, unobservability, and pseudonymity A proposal for terminology. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pages 1–9. Scopus, 2001.

[RB11] M. Rost and K. Bock. Privacy by design and the new protection goals. http://maroki.org/pub/privacy/BockRost_PbD_DPG_en_v1f.pdf, 2011.

[SC09] S. Spiekermann and L. F. Cranor. Engineering Privacy. *IEEE Transactions on Software Engineering*, 35(1):67–82, 2009.

[Sch10] P. Schaar. Privacy by design. *Identity in the Information Society*, 3(2):267–274, 2010.

[SMB96] H. J. Smith, S. J. Milberg, and S. J. Burke. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2):167–196, 1996.

[Sol06] D. J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3):477–564, 2006.

[Spi12] S. Spiekermann. The Challenges of Privacy by Design. *Communications of the ACM*, 55(7):38–40, 2012.

[Uni73] United States Department of Health, Education and Welfare: Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers and the Rights of Citizens: Report*. [Cambridge? Mass.]: [MIT Press], 1973.

[Uni10] United States Federal Trade Commission (FTC). Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers. Technical report. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf, 2010.

[WB90] S. D. Warren and L. D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):193–220, 1890.

[Wri12] D. Wright. The state of the art in privacy impact assessment. *Computer Law & Security Review*, 28(1):54–61, 2012.

[WSJ14] K. Wuyts, R. Scandariato, and W. Joosen. Empirical evaluation of a privacy-focused threat modeling methodology. *The Journal of Systems & Software*, 96:122–138, 2014.