Supporting the Design of Privacy-Aware Business Processes via Privacy Process Patterns

Vasiliki Diamantopoulou
and Nikolaos Argyropoulos
School of Computing, Engineering
and Mathematics
University of Brighton, UK
{v.diamantopoulou,n.argyropoulos}@brighton.ac.uk

Christos Kalloniatis
Department of Cultural Technology
and Communication
University of the Aegean, Greece
chkallon@aegean.gr

Stefanos Gritzalis
Department of Information and
Communication Systems Engineering
University of the Aegean, Greeece
sgritz@aegean.gr

***Abstract*—Privacy is an increasingly important concern for modern software systems which handle personal and sensitive user information. Privacy by design has been established in order to highlight the path to be followed during a system's design phase ensuring the appropriate level of privacy for the information it handles. Nonetheless, transitioning between privacy concerns identified early during the system's design phase, and privacy implementing technologies to satisfy such concerns at the later development stages, remains a challenge. In order to overcome this issue, mainly caused by the lack of privacy-related expertise of software systems engineers, this work proposes a series of privacy process patterns. The proposed patterns encapsulate expert knowledge and provide predefined solutions for the satisfaction of different types of privacy concerns. The patterns presented in this work are used as a component of an existing privacy-aware system design methodology, through which they are applied to a real life system.**

***Keywords*—Privacy Process Patterns, Business Processes, Requirements Engineering, Information Security Modelling.**

I. Introduction

The protection of personal and sensitive information is considered as an important challenge in the domain of Information and Communication Technology (ICT), attracting much attention recently [1], [2]. With an increasing amount of sensitive and confidential information stored, shared and manipulated at the digital level [3], both individuals and organisations expect appropriate measures to ensure the privacy of such information [4]. However, this is not easy, as privacy is a multifaceted concept with various implications and ways of achievement, which depend, among other things, on the environment in which it is required to be achieved.

Privacy is considered as a design criterion that needs to be considered early during the system design phase [5]. The paradigm of Privacy by Design (PbD) has been proposed as a feasible solution for such situation, though there are still major challenges that require further investigation. In particular, a challenging task in the context of PbD is moving from a design (where the privacy requirements of an information system have been elicited) to an implementation that fulfills those requirements [6]. This requires further elaboration for two main reasons. On the one hand, there is little expertise on how best to align privacy requirements (from the design stage) to the use of the appropriate Privacy Enhancing Technologies (PETs) [7] at the implementation stage. On the other hand, software engineers, who need to deal with both the design and the implementation stages, lack detailed knowledge of PETs to ensure their correct implementation.

This paper contributes towards these two challenges by proposing a set of privacy process patterns in order to create a clear alignment between privacy properties (requirements) and PETs, and encapsulate expert knowledge of PET implementation at the operational level. By describing each privacy pattern with a textual template and a business process fragment, system designers without prior expertise in the area of privacy can have a basic overview of the characteristics of each pattern (e.g., problem it resolves, benefits and liabilities of its usage) and a predefined sequence of activities for integrating privacy in the system's processes. Moreover, by integrating the introduced privacy process patterns to PriS [8], a privacy-aware system design framework, we demonstrate how system developers can bridge the gap between design and implementation. Finally, we apply the proposed approach to a real life system to demonstrate its applicability in practice.

The rest of this paper is structured as follows. Section II presents the privacy process patterns through a textual template and a series of business process fragments, in order to define both their individual characteristics and the sequence of activities involved for each privacy process pattern. Section III describes their integration to the PriS methodology. Section IV illustrates an application of the proposed approach to a case study. Section V discusses related work and Section VI concludes the paper by raising issues for further research.

II. Privacy Process Patterns

A pattern, in the context of software development, is a reusable package which incorporates expert knowledge and represents a recurring structure, activity, behaviour or design [9], [10], offering solutions to specific problems. Privacy patterns are considered as a way to model privacy issues. In order to describe the effect of privacy requirements on business processes, and to facilitate the identification of the system architecture that best supports the privacy related business processes [11], we suggest the utilisation of privacy process patterns that can provide a holistic approach from business

978-1-5090-5476-3/17/$31.00

goals to "privacy-compliant" IT systems. Thus, *Privacy Process Patterns are patterns being applied on privacy related processes in order to specify the way that the respective privacy issues will be realised through a specific sequence of steps*. More specifically, in the context of this work, we will focus on design patterns, which have been proposed in many domains as a format for capturing and sharing design knowledge [12], [13]. Design patterns describe, at a mid-level of abstraction, a commonly recurring structure of communicating components that solves a general design problem and is independent of the implementation language used [14], [15]. The privacy process design patterns proposed by this work will be expressed as BPMN process fragments which aim to assist developers to understand, in a better and more structured way, how to implement the various privacy concepts, allowing them to identify the pattern that best fits their particular situation. The use of privacy process patterns is considered as a more robust way for bringing the gap between the design and the implementation phase of a system or module of it [16], [17].

The context in which each of the proposed patterns can be applied is an important aspect that needs to be considered. To provide system developers with relevant information about the structure of each of the proposed patterns, the so-called Alexandrian format [12] will be followed, which is already accepted and used for the definition of security patterns [18]. Through the *definition* field, we provide a comprehensive definition of the privacy concept. The fields *problems* and *forces* present the goals that need to be fulfilled and the forces that need to be considered when choosing to use this pattern, respectively. The fields *benefits* and *liabilities* present the advantages and the disadvantages that are identified in each privacy concept. The field *implementation techniques* covers an indicative set of possible techniques that satisfy the respective concept. From the range of the proposed implementation techniques, the developers can choose the most appropriate technology based on the privacy process patterns applied on every privacy-related process. Finally, the field of *related patterns* indicates which patterns have similar characteristics with the examined one, which patterns are closely related in terms of functionality and with which other patterns it can be utilised.

In addition to the textual description of the proposed privacy patterns, a business process design pattern is provided for each type of privacy concept. Such patterns, modelled in BPMN 2.0 [19], encapsulate business process fragments which aim to guide the operationalisation of privacy at the business process level. Their granularity allows such process patterns to be generic enough to be implementation-agnostic but, at the same time, able to specify a basic sequence of activities and interactions between process participants for the satisfaction of the system's privacy requirements. Therefore, the activities contained within each pattern are not dependent on the implementation of a specific privacy-enhancing technology but rather on the type of the privacy concept they operationalise. As a result, a number of different technologies (e.g., smartcard, biometrics, identity management) implementing the same type of privacy concept (e.g., pseudonymity) can be integrated within the same pattern.

The basic template around which the proposed patterns are modelled includes one sub-process in the system lane, within which the selected privacy mechanism is operationalised, and a corresponding sub-process at the user's lane, where the interaction with the mechanism takes place (e.g., username and password input). Additional activities are also included to capture the communication between the user and system side regarding the success or failure of the operation (e.g., *"Access Granted"*, *"Secure connection established"*). Both of the sub-processes are marked with a padlock symbol at their top left corner to visually communicate that they perform privacy-implementing activities. It is also often the case that parts of a pattern are reused within another pattern.

Early versions of the privacy process fragments have been introduced and evaluated in our previous work [20]. The process patterns presented in this work are the result of an optimisation and refinement process during which some of the existing patterns were combined, while the workflows and activities included in others were defined more precisely. The refinement process was performed in accordance to guidelines for process modelling [21] which suggest minimising the number of activities and workflows, keeping the process structure consistent with BPMN rules and following the correct naming conventions for its activities (verb-object labels).

The patterns described in this work were developed in order to cover the eight privacy concepts, as identified and defined by the consensus of the literature of the area [22], [23], [24], [25], [26], [27], namely *authentication*, *authorisation*, *anonymity*, *pseudonymity*, *unlinkability*, *undetectability*, *unobservability* and *data protection*. The first two are mainly security concepts but they are included due to their key role in the implementation of privacy protection. Moreover, as literature indicates [24], from a technological perspective, some privacy concepts can satisfy others. Thus, as shown by the patterns presented below, anonymity can be achieved by the implementation of pseudonymity, and unobservability requires the implementation of both the anonymity and undetectability. The satisfaction of these privacy concepts leads to the minimisation or elimination of the collection of identifiable user data. Our intention is to define a general template for privacy concepts that can be used to describe other concepts in addition to the eight listed above. This template comprises a guide for developers so they can understand in a better and more structured way how to implement each privacy concept.

A. Authentication

Definition: Provision of assurance that a claimed characteristic of an entity is correct

Problem: Prevention of fraudulent connection requests

Forces: The protection of confidentiality and integrity of the data

Benefits: i) verifies a user's identity, ii) ensures the origin integrity (the source of the data)

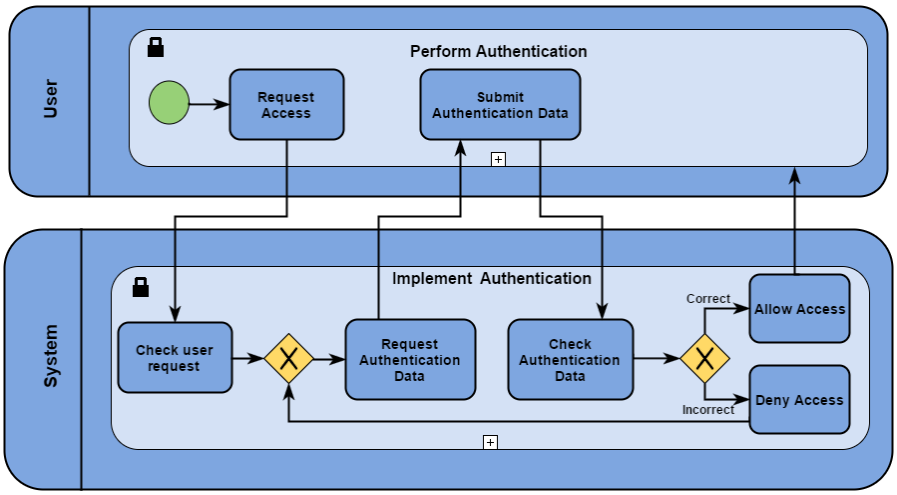

Fig. 1. Authentication process pattern

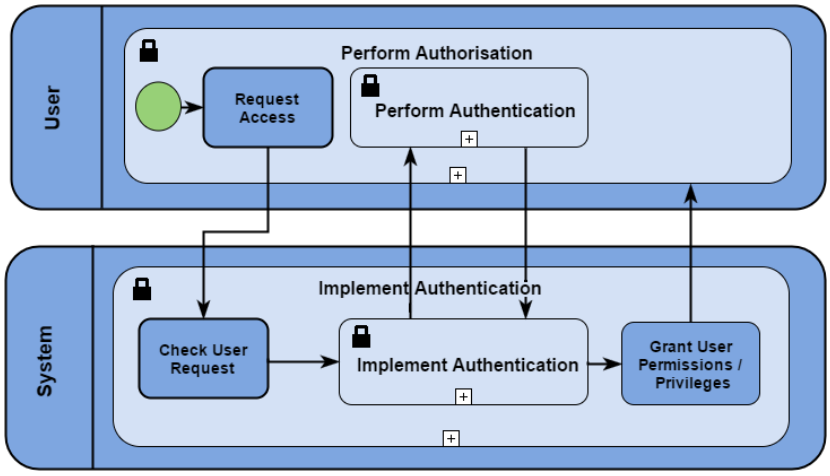

Fig. 2. Authorisation process pattern

Liabilities: i) computer resources for the implementation and execution of authentication security mechanisms are required, ii) complicated implementation and debugging, iii) a single point of failure. If the mechanism fails, the security of the system is in danger

Implementation techniques:

- Administrative tools: Identity management, biometrics [28], smart cards [29], permission management
- Information tools: Monitoring and audit tools

Related patterns: Authorisation

B. Authorisation

Definition: User's private data should only be accessed by authorised users

Problem: The description of allowable types of accesses (authorisations) by active computational entities (subjects) to passive resources (protection objects)

Forces: i) definition of the access policies for resources, ii) structure independent of the type of resources. The description of the access must be in a uniform way, iii) predicates or guards may restrict the use of the authorisation according to specific conditions

Benefits: i) allows an authenticated client to use a particular service, ii) deters violations of the integrity of either the systems or users resources, iii) deters violations of privacy

Liabilities: i) applies various limitations on user access or actions, requires users to log on separately to each system or service that they want to access, ii) Administrative overheads

Implementation techniques:

- Administrative tools: Identity management, biometrics, smart cards, permission management
- Information tools: Monitoring and audit tools

Related patterns: Authentication

C. Anonymity

Definition: Anonymity is a characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly. During anonymization, identity information is either erased or substituted

Problem: The user of a service cannot be identified

Forces: Large number of users in the same network is required

Benefits: i) supports users in accessing services without disclosing their identity, ii) users are more freely expressed, since freedom from user profiling is achieved (behaviour of users or other privacy-infringing practices), iii) freedom from location tracking, iv) minimal user involvement (they do not have to modify their normal activities for anonymity services)

Liabilities: i) maintain users' accountability while anonymous, ii) performance (latency, loss of functionality, bandwidth, etc.), iii) usability of information (too much data obfuscation can undermine the usefulness of data), iv) abuse of privacy (malicious users), v) user count (large anonymity set), vi) user friendliness (if the users have to adapt a lot to achieve anonymity, they may start judging where they should have anonymity), vii) law enforcement (the anonymity might have to be liftable to investigate on crime suspects)

Implementation techniques:

- Anonymizer products, services and architectures: Browsing pseudonyms [30], Virtual Email Addresses, Trusted third parties, Crowds [31], Onion routing[32], DC-nets [33], Mix-nets (Mix Zone) [34], Hordes [35], GAP [36], Tor [37], Aggregation Gateway [38], Dynamic Location Granularity
- Track and evident erasers: Spyware detection and removal, Hard disk data eraser, User data confinement pattern, Use of dummies

Related patterns: Pseudonymity, unlinkability

D. Pseudonymity

Definition: Pseudonymity is the utilisation of an alias instead of personally identifiable information

Problem: Ensuring that an entity cannot be linked with a real identity during online interactions

Forces: Use authenticated services without disclosing identifiable information

Benefits: i) supports users in accessing services without disclosing their real identity, ii) permits the accumulation of reputational capital, iii) the user is still accountable for its actions, iv) a user may have a number of pseudonyms, v) fills the gap between accountability and anonymity, vi) hides the identity of the participants, vii) prevents unforeseen ramifications of the use of online services

Liabilities: i) maintains users' accountability while pseudonymous, ii) abuse of privacy (malicious users), iii) forgery/impersonation, iv) law enforcement (the anonymity might have to be liftable to investigate on crime suspects), v) extensive usage of the same pseudonym can weaken it

Implementation techniques:

- Administrative tools: Identity management, Biometrics, Smart cards, Permission management
- Pseudonymizer tools: CRM personalisation [39], Application data management, Obligation management, Mixmaster

Related patterns: Anonymity, authentication

E. Unlinkability

Definition: Unlinkability is the use of a resource or a service by a user without a third party being able to link the user with the service

Problem: i) users' identifiable information is not protected, ii) the strength of unlinkability is depended on the number of nodes belonging to the unlinkability set

Forces: Enforce users' privacy regarding the linkability with the service used

Benefits: i) protect users' privacy when using a resource or service by not allowing malicious third parties to monitor which services are used by the user, ii) the intentional severing of the relationships (links) between two or more data events and their sources, ensures that a user may make multiple uses of resources or services without others being able to link the uses together, iii) requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system, iv) minimise risks to the misuse of the privacy-relevant data and to prohibit or restrict profiling

Liabilities: i) maintain a large unlinkability set, ii) equal distribution of traffic between the potential senders and the potential recipients, iii) unidirectional pseudonyms should be preferred because omnidirectional pseudonyms are susceptible to profiling

Implementation techniques:

- Anonymizer products, services and architectures: Trusted third parties, Surrogate keys, Onion routing, DC-nets, Mix-nets, Hordes, GAP, Tor, Aggregation Gateway
- Pseudonymizer tools: CRM personalisation, Application data management
- Track and evident erasers: Spyware detection and removal, Browser cleaning tools [40], Activity traces eraser, Hard disk data eraser, Use of dummies, Identity Federation Do Not Track Pattern

Related patterns: Undetectability, anonymity

F. Undetectability

Definition: Undetectability is the inability for a third party to distinguish who is the user (among a set of potential users) using a service

Problem: The strength of undetectability depends on the number of nodes belonging to the undetectability set

Forces: Enforce users' privacy by allowing them to use a service without being detected by a malicious third party

Benefits: i) protect users' privacy when using a resource or service by not allowing malicious third parties to detect which services are used by the user, ii) the attacker cannot sufficiently detect whether a particular Item of Interest (IOI) exists or not, e.g. steganography, iii) the attacker cannot sufficiently distinguish whether it exists or not.

Liabilities:

- Maintain a large undetectability set
- Equal distribution of traffic between the potential senders and the potential recipients

Implementation techniques:

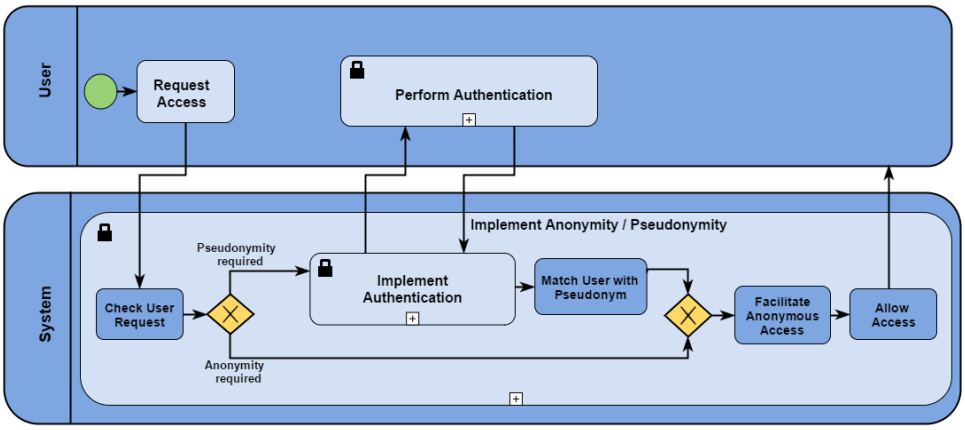

Fig. 3. Anonymity and Pseudonymity process pattern

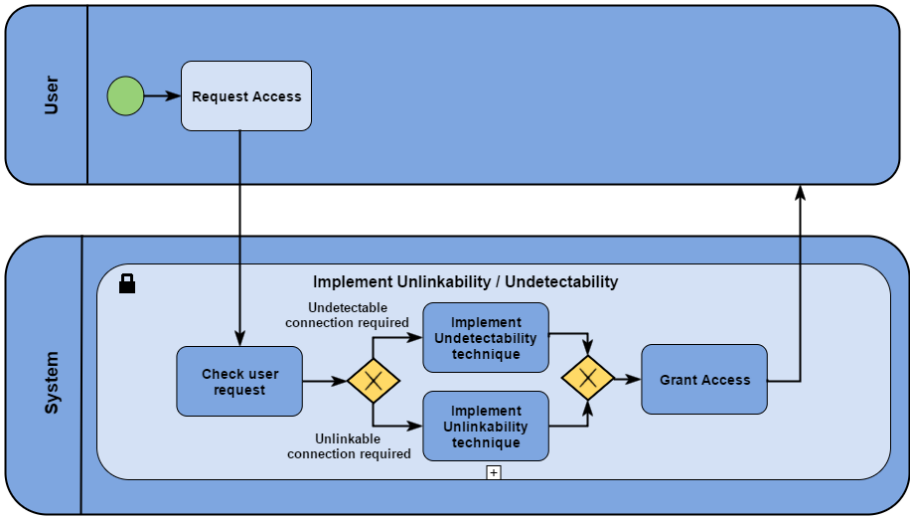

Fig. 4. Unlinkability and Undetectability process pattern

- Administrative tools: Smart cards, Permission management
- Information tools: Monitoring and audit tools
- Anonymizer products, services and architectures: Hordes, GAP, Tor
- Track and evidence erasers: Spyware detection and removal, Browser cleaning tools, Activity traces eraser, Hard disk data eraser, Identity Federation Do Not Track Pattern
- Encryption tools: Encrypting email [41], Encrypting transactions [42], Encrypting documents

Related patterns: Unlinkability, unobservability

G. Unobservability

Definition: Unobservability is the inability of a third party to observe if a user (among a set of potential users) is using a service

Problem: The strength of unobservability set depends on the strength of: i) the sender/recipient anonymity set, ii) the sender/recipient undetectability set

Forces: Users privacy is enforced since they can use a resource or service anonymously and without being detected regarding the service used when the state of IOIs should be indistinguishable from any IOI (of the same type) at all when we want to send messages that are not discernible from e.g. random noise.

Benefits: i) anonymity and Undetectability enforcement per service, ii) ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used, iii) requires that users and/or subjects cannot determine whether an operation is being performed.

Liabilities: i) depends on the successful implementation of both anonymity and undetectability, ii) strong encryption required demanding many resources, iii) slower communication due to complex calculations

Implementation techniques:

- Administrative tools: Smart cards, Permission management
- Anonymizer products, services and architectures: Hordes,

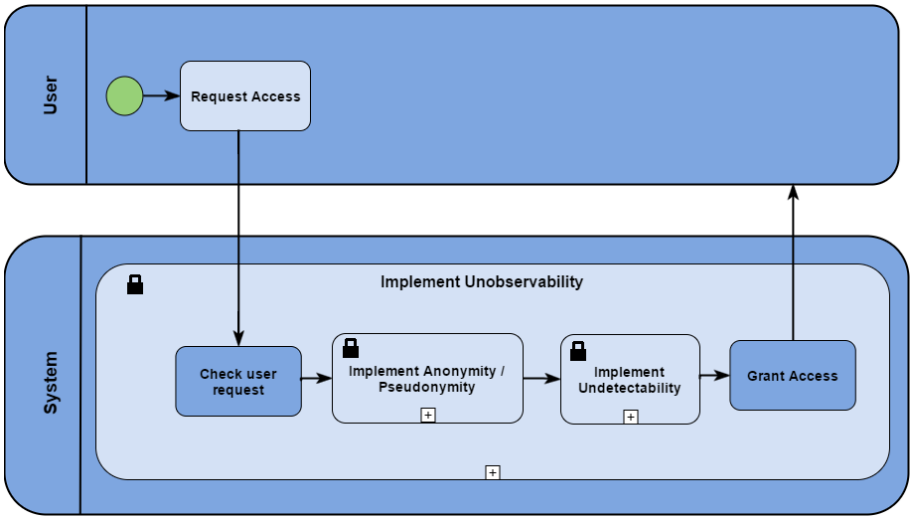

Fig. 5. Unobservability process pattern

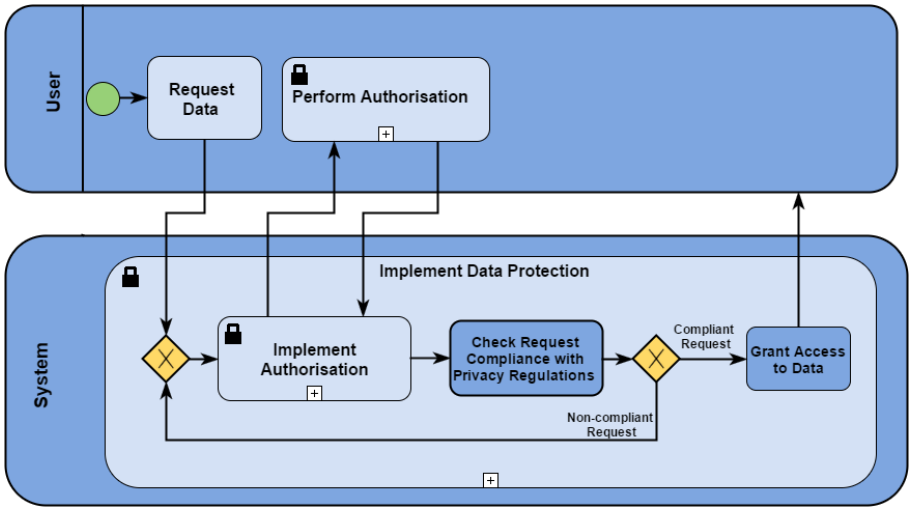

Fig. 6. Data Protection process pattern

GAP, Tor

- Track and evidence erasers: Spyware detection and removal, Hard disk data eraser, Identity Federation Do Not Track Pattern

Related patterns: Anonymity, undetectability

H. Data protection

Definition: The protection of personal data in order to guarantee privacy

Problem: No individual without authorisation can access the users data

Forces: Every transaction with personal data is realised according to the system's privacy regulations and GDPR [43] regarding the processing of personal data and the free movement of such data

Benefits: i) ensures the integrity of the data, ii) protects the data from corruption, manipulation, loss, or errors, iii) empowers individuals to control their information

Liabilities: i) complexity of the adaptation, ii) it is not the primary requirement of a system and it may even come into conflict with other (functional or non-functional) requirements

Implementation techniques:

- Administrative tools: Identity management, biometrics, smart cards, permission management
- Information tools: Monitoring and audit tools, privacy policy generators, privacy policy readers, privacy compliance scanning
- Encryption tools: Encrypting documents

Related patterns: Authentication, Authorisation

III. Privacy Process Pattern Integration through PriS Methodology

The implementation of the aforementioned privacy process patterns follows an abstract approach, enabling them to be applied to any requirements engineering methodology. In order

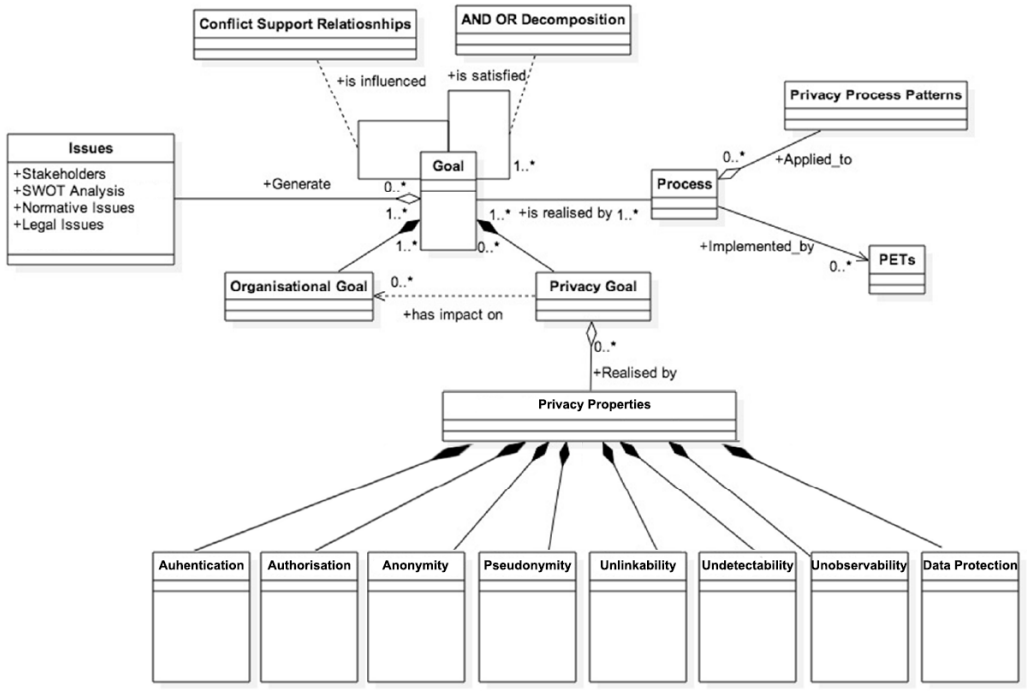

Fig. 7. Conceptual model

to substantiate the applicability and usefulness of the privacy process patterns that have been presented in Section II, we opted to apply them on an established privacy requirements engineering methodology, called PriS (Privacy Safeguard) [44]. This methodology incorporates privacy requirements into the system design process and has been developed so as to assist designers on eliciting, modelling and designing privacy requirements of the system to be, and also to provide guidance to the developers on selecting the appropriate implementation technique(s) that best fit the organisation's privacy requirements. PriS provides a set of concepts for modelling privacy requirements in the organisation domain and a systematic way-of-working for translating these requirements into system models, adopting the use of privacy process patterns as a way to i) describe the effect of privacy requirements on business processes and ii) facilitate the identification of the system architecture that best supports the privacy-related business processes [45].

The PriS methodology comprises the following four activities that are presented below in an abstract way, as the implementation of them will be thoroughly described in Section IV, through a real case study:

1) *Elicit privacy-related goals*. This step concerns the elicitation of the privacy goals that are relevant to a specific organisation. It usually involves a number of stakeholders and decision makers (managers, policy makers, system developers, system users, etc.).
2) *Analyse the impact of privacy goals on organisational processes*. The second step is to analyse the impact of these privacy goals on processes and related support systems.
3) *Model affected processes using privacy process patterns*. Having identified the privacy-related processes, the next step is to model them, based on the relevant privacy process patterns.
4) *Identify the technique(s) that best support/implement the above process*. The final step is to define the system architecture that best supports the privacy-related process identified in the third step. Again, the defined privacy process patterns are used to identify the proper implementation technique(s) that best support/implement corresponding processes.

The proposed methodology uses the concept of *goal* as the central and most important concept. Goals are desired state of affairs that need to be attained. Goals concern *stakeholders*, i.e. anyone that has an interest in the system design and usage. Also, goals are generated because of issues. An *issue* is a statement of a strength, weakness, opportunity or threat that leads to the formation of the goal. Privacy is a highly regulated area in Europe. The protection of users' privacy is stated in many European and national legislations through the form of laws, policies, directives, best practices, etc. [43]. Thus, *legal issues* need to be taken under consideration during the identification of functional and non-functional requirements. Goal identification needs to take under consideration all these elements before further analysis is conducted.

As shown in Fig. 7, there are two types of goals in the proposed methodology, namely *organisational goals* and *privacy goals*. Organisational goals express the organisation's main objectives that need to be satisfied by the system into

consideration. In parallel, privacy goals are introduced because of specific *privacy related concepts*. Through privacy goals, the *realisation* of the identified privacy concepts is achieved. Thus, all privacy related concepts that need to be realised should be addressed as specific privacy goals. Privacy goals may have an *impact* on organisational goals. In general, a privacy goal may cause the improvement/adaptation of organisational goals or the introduction of new ones. In this way, privacy issues are incorporated into the system's design. Every model has at least one organisational goal, but may have no privacy goals, thus the respective cardinality relationships (1..* and 0..*) among the organisational and privacy goal with the generic concept of goal. Goals are realised by *processes*. The relationship between goals and processes is many to many, in the sense that one goal can be realised from one or more processes and one process can support the realisation of one or more goals.

IV. Illustration of Privacy Process Pattern Application

In order to clearly demonstrate how the proposed privacy patterns can be applied during the design of a real-life system, we provide a case study. The system selected for this case study, in which the PriS methodology has already been implemented to, involves the University of the Aegean Career Office Unit. More specifically, the University of the Aegean has built a software system for its Aegean Career Office. A detailed description of the Career Office System can be found in [46]. The scope of this case study was the identification of all respective concepts, using the PriS framework for conducting privacy-aware analysis based on the system's context and the stakeholders' requirements. The main objective of the Career Office system of the University of the Aegean is boundary management, i.e. helping students to manage the choices and transitions they need to make on exit from their studies in order to proceed effectively to the next step of their life. The Career Office system follows three main principles that form the three primary organisational goals namely: a) Provide Career Information, b) Offer Guidance through Events and c) Maintain a lifelong communication with the graduates. In Fig. 8 the goal model of the examined case study is depicted. The authors decided to analyse only the principle "Maintain a lifelong communication with the graduates", for simplicity reasons.

A. PriS application

In accordance with the *first step* of PriS, the main privacy requirement identified along with stakeholders, was the following: "Graduates' anonymity should be enforced when collecting the completed questionnaires". For protecting graduates' privacy, it is of major importance to ensure that all types of analysis and produced results don't lead to any form of privacy violation, directly or indirectly. Based on the organisation's context, the Career Office must ensure graduates that nobody, especially malicious third parties, will be able to reveal the name, or other elements, that may lead to the identification of the graduate that submits the answered questionnaire; when graduates send information through the career office portal, it must be ensured that others will not be able to reveal any personal identifiable information. Following the identified requirement, the privacy goal that needs to be addressed and fulfilled is the anonymity goal.

Proceeding to the *second step* of PriS methodology, the impact of this goal in the Career Office system has to be identified, and thus, the identification of the organisational goals and subgoals that deal with the specific requirement is of utmost importance. For satisfying the anonymity goal, the main goal, subgoal and process affected are the following:

- Main Goal: Maintain a lifelong communication with the graduates (G3)
- Subgoal: Make follow up research concerning the professional progress of the graduates by sending them questionnaires (G 3.3)
- Main Process: Conduct Graduates Surveys (P4)
- Subprocess: Analyse Responses (P 4.3)

The *third step* of PriS indicates the modelling of the affected processes, using privacy process patterns. For realising the identified privacy goals, the respective processes that implement the privacy-related subgoals were identified. Thus, for the anonymity goal, the respective process that identifies the operationalised subgoal G3.3 is P4 and specifically, "P4.3 Analyse Responses". For assisting the realisation of privacy goals on processes, privacy process patterns are introduced. More specifically, for every privacy goal, a respective privacy process pattern may be introduced into the processes, leading to the realisation of the privacy requirements by the respective PET.

The business process model for P4 ("Conduct Graduates Survey") is presented in Fig. 9. All the subprocesses of P4, except P 4.3, are presented as collapsed sub-processes due to space limitations. The P 4.3 subprocess ("Analyse Responses") is presented as expanded sub-process in order to illustrate how the process pattern for anonymity can be integrated within the rest of its activities. In particular, the anonymity pattern, as presented in Fig. 3, is interjected before a graduate can submit a completed survey questionnaire to the university's Career Office system. The system checks the request and proceeds with the decision of preserving user's anonymity (in case the type of service requested should satisfy this privacy goal) or executes the authentication task, as captured by the Authentication process pattern (Fig. 1), which leads the user to the process of providing their credentials for gaining access to use the requested service via a pseudonym. Next, the system creates an anonymous connection, by using one of the suggested PETs, via which the graduates can submit their survey forms. Thus, by applying the relevant privacy process pattern on the respective privacy-related process, it is easier for the designer to identify both the appropriate PETs and the sequence of activities required for their integration to the rest of the process, leading to the satisfaction of the respective system goals.

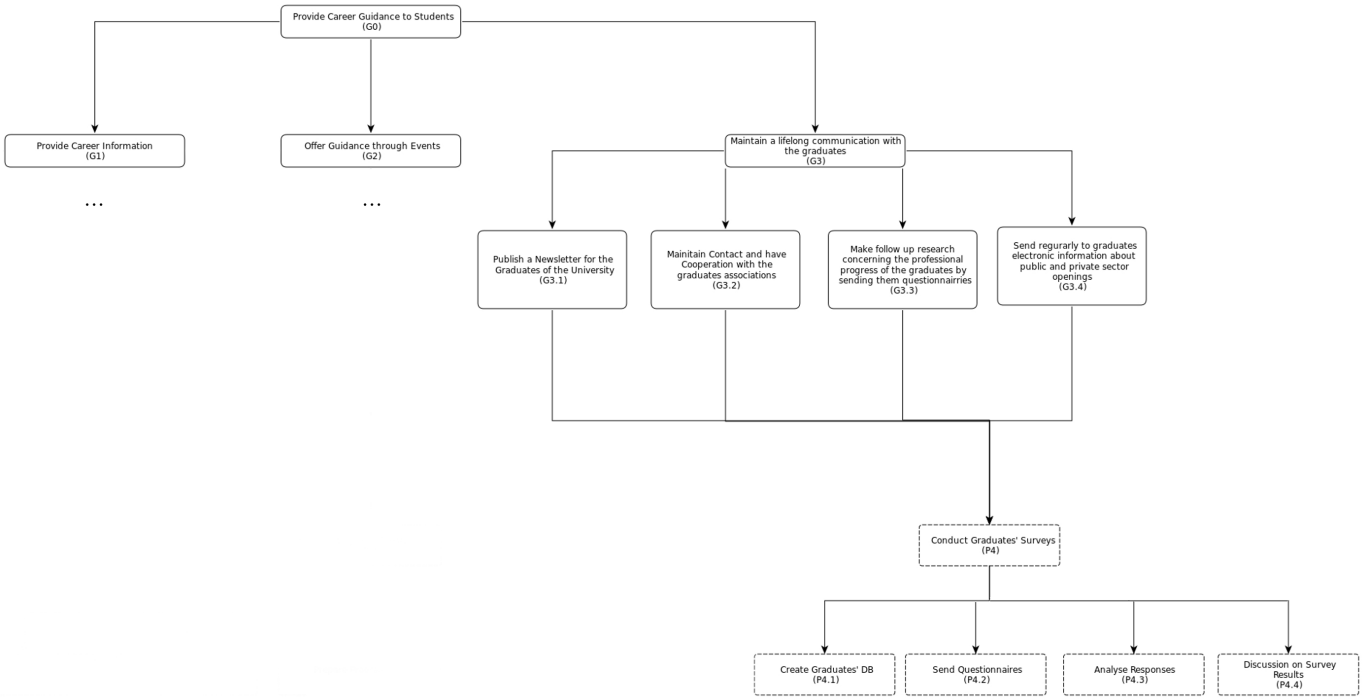

Fig. 8. Goal model

Finally, according to the *fourth* and final step of PriS, the technique(s) that best support/implement the above mentioned procedures have to be identified. Thus, the designer along with the stakeholders and the organisation's developer team decide and propose the most appropriate PET for realising the identified privacy goals. The definition of selection criteria for the most adequate PET is out of the scope of this paper. In the given scenario, from the different options presented in Section II, our analysis has identified and suggested to the stakeholders the following PETs: *Crowds*, *Onion Routing*, *Tor* and *GAP Protocol*.

B. Discussion

The application of the PriS methodology, enhanced with the privacy process patterns presented in this work, allowed us to gain useful insights. In terms of applicability, the proposed patterns were easily integrated into the existing business process model. This can be attributed to both the ability of PriS to pinpoint, through its analysis, the specific part of the process where the privacy process pattern should be applied, and the structure of the patterns themselves, which are expressed at a process workflow level of abstraction. Therefore, having a structured approach for identifying where a pattern should be applied and a set of patterns operating at the appropriate level of abstraction, enhances their applicability.

The application presented above was performed in a system relatively simple in terms of size and complexity. The addition of the privacy process patterns into the existing business process resulted in an increase to the overall complexity of the model, mainly due to the fact that the anonymity pattern introduces a number of extra activities and sub-processes, since it also requires the implementation of authentication. Nevertheless, since the structure of the patterns is predefined and minimal adjustments are required for their instantiation within a process model, the amount of manual intervention required for their integration is relatively low. Nonetheless, a more complete evaluation of the scalability of the approach will be provided by its application to a larger scale case study, as part of our future work.

Overall, the advantage of the proposed approach, as illustrated by its application, is the provision of a well-defined set of actions, which system designers, without specialised knowledge of privacy, can utilise for the incorporation of privacy implementing technologies in business processes. The abstraction of the proposed set of patterns makes them flexible enough to accommodate their instantiation by different types of privacy enhancing technologies (PETs) and facilitates reusability, as the same pattern can be instantiated by a different PET if the system needs to be reconfigured. Nevetheless, there are also aspects of the proposed work which need to be further developed, mainly in regards to combinations of different patterns for the satisfaction of complex privacy requirements while maintaining a manageable modelling complexity. Another aspect that would strengthen the usability of our approach is the development of CASE tools, to minimise the effort required for incorporating the proposed patterns into business process models, and the integration of decision support functionalities, in order to facilitate the selection of the appropriate PETs for instantiating the patterns according to specific system needs.

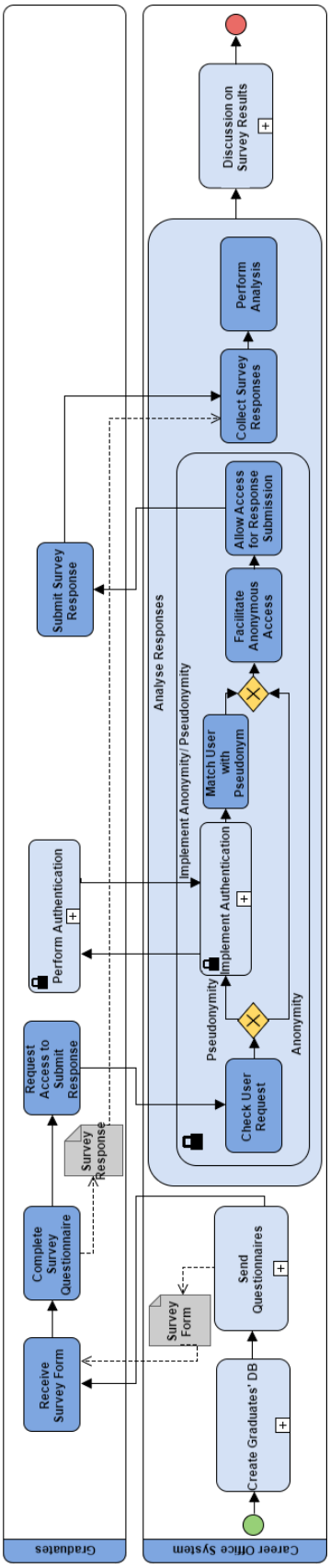

Fig. 9. Business Process model for Conducting Graduates Survey

V. Related Work

Patterns have been adopted into software engineering as they encounter each problem in a systematic and structured way. In particular, privacy patters have been used as a way to model privacy issues. Since recent research has identified that privacy should be treated as a separate requirement criterion [47], [48], [49], the need for the identification of patterns focusing on solving privacy issues is imperative.

So far, literature provides some examples of privacy patterns. In [50] three privacy patterns have been implementing, focusing on web-based activity and especially for conveying privacy policies to end-users during online interactions, protecting individuals from jeopardy. These patterns benefit online organisations, website designers and users, since they are able to ensure appropriate disclosure and use of personal information when the latter is exposed to online environments. The authors in [51] have identified 45 design patterns, demonstrating how the application of their proposed patterns can accelerate the development process to produce a better overall design. They have focused in ubiquitous computing environments and among the patterns they present, 15 of them are focused on privacy related issues. The authors in [52] propose a pattern language which contains 12 patterns for developing anonymity solutions for various domains, including anonymous messaging, anonymous voting and location anonymity. This work moves on the right direction regarding the modelling of privacy requirements but it fails to combine privacy elicitation concepts for capturing privacy requirements. In [53], six patterns that focus on how to establish boundaries for interaction are presented, focusing on the filtering of personal information in collaborative systems. Finally, the author in [54] presented two privacy patterns, applying this approach to security issues by proposing a set of security patterns to be applied during the software development process. The aforementioned works contribute to the growing privacy patterns library, each of them covering a specific domain. Our work provides a series of guidelines to be used by system designers to implement privacy requirements, as established by the literature of the area, facilitating the bridging of the gap between the design and implementation phases.

In the context of business process modelling, patterns have been utilised for encapsulating expert knowledge on the operationalisation of security and privacy concerns. In [15] a textual template is followed to describe different aspects of security patterns (e.g., problem description, solution description, related patterns, and more), which capture the functionality of security implementing techniques and mechanisms (e.g., password authentication, encrypted storage). The work presented in [55] introduces SecBPMN, a framework for the design of secure socio-technical systems which uses SecBPMN-ml, an extension of BPMN, for the annotation of security on elements of the business process models. Each type of security requirement is also described by a series of predicates which, similar to security process patterns, encapsulate security-related information in the context of the

business process. Focusing exclusively on privacy, in [45], [44] the PriS framework is introduced for the incorporation of privacy requirements into business process designs. A series of activity diagrams abstractly describe the activities required for the integration of PETs in the final business processes. These privacy-related process patterns, introduced by PriS, are further refined and expressed as BPMN 2.0 process fragments in [20].

VI. Conclusions

The protection of users' privacy is an increasingly important aspect of information systems. Nevertheless, during the design of such systems, privacy is usually considered as an afterthought due to the lack of expertise of system designers and developers. Even if privacy concerns are identified during the early design phases, another obstacle that arises is the selection and implementation of appropriate privacy enhancing techniques during the development of the system.

A contribution towards overcoming such challenges, in the form of structured privacy process patterns has been presented in this work. More specifically, this paper presented a set of privacy process patterns that can be used to bridge the gap between privacy design and implementation, providing novices with a systematic and structured way to rely on expert knowledge for resolving privacy related issues. The examined patterns are accompanied by business process design patterns expressed in BPMN 2.0, thus capturing the sequence of activities required for the operationalisation of privacy at the business process level. These patterns have also been integrated to the PriS framework which can support the design of privacy-oriented processes, using as input high abstraction-level goal models. The application of the framework is illustrated using the University of the Aegean Career Office system. The steps introduced by PriS were applied to this system along with the respective, newly introduced privacy process patterns in order to create, as the final output, a process model that satisfies the identified privacy requirements.

The integration of the privacy process patterns at the business process of the Career Office system was seamless, as they were captured at the same level of granularity as the rest of the system's process. As a result, the operationalisation of privacy in the Career Office's system did not require high effort, as there was no need for significantly modifying neither the privacy process patterns nor the Career Office's business process for creating a coherent final output.

Future directions of this work include the development of an extended privacy pattern language that will further assist developers into bridging the gap between design and implementation. Moreover, we are planning to extend our work to elicit and define privacy patterns in emerging domains such as Cloud Computing and the Internet of Things.

Acknowledgement

This research was partially supported by the Visual Privacy Management in User Centric Open Environments (VisiOn) project, supported by the EUs Horizon 2020 programme, Grant agreement No 653642.

References

[1] L. Rainie, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish, "Anonymity, privacy, and security online," *Pew Research Center*, vol. 5, 2013.

[2] E. Commission, "Eurobarometer 431 - data protection report," Tech. Rep., 2015.

[3] G. T. Duncan, R. W. Pearson *et al.*, "Enhancing access to microdata while protecting confidentiality: Prospects for the future," *Statistical Science*, vol. 6, no. 3, pp. 219–232, 1991.

[4] PwC, "Moving forward with cybersecurity and privacy - how organizations are adopting innovative safeguards to manage threats and achieve competitive advantages in a digital era," Key findings from The Global State of Information Security Survey 2017, Tech. Rep., 2017.

[5] A. Cavoukian, "Privacy by design [leading edge]," *IEEE Technology and Society Magazine*, vol. 31, no. 4, pp. 18–19, 2012.

[6] S. Gürses, C. Troncoso, and C. Diaz, "Engineering privacy by design," *Computers, Privacy & Data Protection*, vol. 14, no. 3, 2011.

[7] R. Hes and J. Borking, "Privacy enhancing technologies: the path to anonymity," *ISBN*, vol. 90, no. 74087, p. 12, 1998.

[8] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Pris methodology: incorporating privacy requirements into the system design process," in *Proceedings of the SREIS 2005 13th IEEE International Requirements Engineering Conference–Symposium on Requirements Engineering for Information Security, J. Mylopoulos, G. Spafford (Eds.)*, 2005.

[9] E. Gamma, *Design patterns: elements of reusable object-oriented software*. Pearson Education India, 1995.

[10] N. Yoshioka, H. Washizaki, and K. Maruyama, "A survey on security patterns," *Progress in informatics*, vol. 5, no. 5, pp. 35–47, 2008.

[11] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Using privacy process patterns for incorporating privacy requirements into the system design process," in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*. IEEE, 2007, pp. 1009–1017.

[12] C. Alexander, *A pattern language: towns, buildings, construction*. Oxford University Press, 1977.

[13] J. O. Borchers, "A pattern approach to interaction design," *Ai & Society*, vol. 15, no. 4, pp. 359–376, 2001.

[14] D. G. Rosado, C. Gutiérrez, E. Fernández-Medina, and M. Piattini, "Security patterns and requirements for internet-based applications," *Internet research*, vol. 16, no. 5, pp. 519–536, 2006.

[15] D. M. Kienzle and M. C. Elder, "Security patterns for web application development," *University of Virginia technical report*, 2002.

[16] L. Compagna, P. El Khoury, A. Krausová, F. Massacci, and N. Zannone, "How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns," *Artificial Intelligence and Law*, vol. 17, no. 1, pp. 1–30, 2009.

[17] L. Compagna, P. E. Khoury, F. Massacci, R. Thomas, and N. Zannone, "How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach," in *Proceedings of the 11th international conference on Artificial intelligence and law*. ACM, 2007, pp. 149–153.

[18] H. Mouratidis, M. Weiss, and P. Giorgini, "Security patterns meet agent oriented software engineering: a complementary solution for developing secure information systems," in *International Conference on Conceptual Modeling*. Springer, 2005, pp. 225–240.

[19] Object Management Group, "Business Process Model and Notation (BPMN) 2.0," Tech. Rep., 2011.

[20] N. Argyropoulos, C. Kalloniatis, H. Mouratidis, and A. Fish, "Incorporating privacy patterns into semi-automatic business process derivation," in *Research Challenges in Information Science (RCIS), 2016 IEEE Tenth International Conference on*. IEEE, 2016, pp. 1–12.

[21] J. Mendling, H. A. Reijers, and W. M. van der Aalst, "Seven process modeling guidelines (7pmg)," *Information and Software Technology*, vol. 52, no. 2, pp. 127–136, 2010.

[22] S. Fischer-Hübner, *IT-security and privacy: design and use of privacy-enhancing security mechanisms*. Springer-Verlag, 2001.

[23] J. Cannon, *Privacy: what developers and IT professionals should know*. Addison-Wesley Professional, 2004.

[24] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[25] ISO/IEC, "29100:2011(e) information technology - security techniques - privacy framework," Tech. Rep., 2011.

[26] ISO/CEI, "27000:2014(e) information technology - security techniques - information security management systems - overview and vocabulary," Tech. Rep., 2014.

[27] B. Matt *et al.*, *Introduction to computer security*. Pearson Education India, 2006.

[28] A. Jain, P. Flynn, and A. A. Ross, *Handbook of biometrics*. Springer Science & Business Media, 2007.

[29] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in pervasive computing*. Springer, 2004, pp. 201–212.

[30] E. Gabber, P. B. Gibbons, Y. Matias, and A. Mayer, "How to make personalized web browsing simple, secure, and anonymous," in *International Conference on Financial Cryptography*. Springer, 1997, pp. 17–31.

[31] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for web transactions," *ACM Transactions on Information and System Security (TISSEC)*, vol. 1, no. 1, pp. 66–92, 1998.

[32] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing," *Communications of the ACM*, vol. 42, no. 2, pp. 39–41, 1999.

[33] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

[34] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[35] C. Shields and B. N. Levine, "A protocol for anonymous communication over the internet," in *Proceedings of the 7th ACM conference on Computer and communications security*. ACM, 2000, pp. 33–42.

[36] K. Bennett and C. Grothoff, "Gap–practical anonymous networking," in *International Workshop on Privacy Enhancing Technologies*. Springer, 2003, pp. 141–160.

[37] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," DTIC Document, Tech. Rep., 2004.

[38] T. Akers, B. Ware, W. Zheng, M. Kostet, and B. Clark, "Service aggregation gateway," Oct. 19 2006, uS Patent App. 11/551,066.

[39] M. D. Mulvenna, S. S. Anand, and A. G. Büchner, "Personalization on the net using web mining: introduction," *Communications of the ACM*, vol. 43, no. 8, pp. 122–125, 2000.

[40] M. A. Himmel and H. Rodriguez, "Method and apparatus for selective caching and cleaning of history pages for web browsers," Sep. 17 2002, uS Patent 6,453,342.

[41] A. Bacard, *Computer Privacy Handbook: A Practical Guide to E-Mail Encryption, Data Protection, and PGP Privacy Software*. Peachpit press, 1995.

[42] J. R. Wells and E. P. Felt, "System and method for message encryption and signing in a transaction processing system," Apr. 22 2008, uS Patent 7,363,495.

[43] E. Parliament. (2016) Regulation (eu) 2016/679 of the european parliament and of the coucil of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/

[44] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the pris method," *Requirements Engineering*, vol. 13, no. 3, pp. 241–255, 2008.

[45] ——, "Using privacy process patterns for incorporating privacy requirements into the system design process," in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*. IEEE, 2007, pp. 1009–1017.

[46] ICTE-PAN, "Methodologies and tools for building intelligent collaboration and transaction environments in public administration networks," in *Project Deliverable D 3.1b*. University of the Aegean.

[47] S. Gritzalis, "Enhancing web privacy and anonymity in the digital era," *Information Management & Computer Security*, vol. 12, no. 3, pp. 255–287, 2004.

[48] R. Koorn, H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen, and J. Borking, "Privacy enhancing technologies, white paper for decision makers," *Ministry of the Interior and Kingdom Relations, the Netherlands*, 2004.

[49] H. Mouratidis, C. Kalloniatis, S. Islam, M.-P. Huget, and S. Gritzalis, "Aligning security and privacy to support the development of secure information systems." *J. UCS*, vol. 18, no. 12, pp. 1608–1627, 2012.

[50] S. Romanosky, A. Acquisti, J. Hong, L. F. Cranor, and B. Friedman, "Privacy patterns for online interactions," in *Proceedings of the 2006 conference on Pattern languages of programs*. ACM, 2006, p. 12.

[51] E. S. Chung, J. I. Hong, J. Lin, M. K. Prabaker, J. A. Landay, and A. L. Liu, "Development and evaluation of emerging design patterns for ubiquitous computing," in *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*. ACM, 2004, pp. 233–242.

[52] M. Hafiz, "A pattern language for developing privacy enhancing technologies," *Software: Practice and Experience*, vol. 43, no. 7, pp. 769–787, 2013.

[53] T. Schümmer, "The public privacy–patterns for filtering personal information in collaborative systems," in *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, 2004.

[54] M. Schumacher, "Security patterns and security standards." in *EuroPLoP*, 2002, pp. 289–300.

[55] M. Salnitri, F. Dalpiaz, and P. Giorgini, "Designing secure business processes with secbpmn," *Software & Systems Modeling*, pp. 1–21, 2016.