Enterprise Architecture Patterns for GDPR Compliance

Clara Teixeira
Supervisors: André Vasconcelos and Pedro Sousa
Instituto Superior Técnico, Avenida Rovisco Pais 1, Lisbon, Portugal
{clara.teixeira, andre.vasconcelos, pedro.sousa}@tecnico.ulisboa.pt,

Keywords: GDPR, Compliance, Personal Data, Enterprise Architecture Patterns.

Abstract: With the growth of technology and the personalization and customization of the internet experiences, personal data has been stored and processed more and more. In some cases, the data subject has not agreed with the retrieval and the purpose of the processing. To solve this, the European Union (EU) parliament approved the General Data Protection Regulation (GDPR), a regulation that has the data subjects' interests in mind. Since some of the concepts and requirements are hard to comprehend, patterns can help system architects and engineers to deliver GDPR compliant information systems. It is important to emphasize that these privacy-related concerns should be addressed at a design level, not after the implementation. This methodology is mostly known as privacy by design. This work focuses on the requirements brought by the GDPR and in providing enterprise architecture patterns to achieve GDPR compliance by proposing a library of patterns. This library is organized in 11 use cases with the GDPR principles that they address; it has 22 patterns, each one handling one or more use cases, modeled in ArchiMate, for a clearer understanding of the solutions. The patterns are applied to a case study, and the impacts are assessed.

1 INTRODUCTION

The importance of securing clients' and employees' personal information has always been evident. However, the growth of technology and the need to ensure that data is safely stored required a common regulation (Intersoft Consulting, 2020). Although several countries already had some legislation regarding this issue, it was not the same for everyone; some countries had an easy adaption, and others had to start from the ground. Companies and other organizations had to question: "How do we achieve GDPR compliance?". To answer this question, the requirements brought by the GDPR and the steps needed for compliance were collected and analyzed. Nevertheless, only knowing what is new is not enough; what would be helpful is to know how to achieve this compliance. By reading the regulation, we have an idea about the changes but not a solution to address those changes, and here is where patterns appear!

According to Alexander, et al. (1977), "each pattern describes a problem which occurs over and over again in our environment, and then describes the core of the solution to that problem, in such a way that you can use this solution a million times over, without ever doing it the same way twice." and are used in different domains, like meta-programming, games, etc. Since patterns provide solutions for recurring problems and can be used multiple times, they are a perfect tool to solve the constraints brought by the GDPR. Unfortunately, in the regulation itself, these new concerns do not come with "how to's" for its implementation in projects and services; but the patterns can help. This work aims to identify relevant patterns that can provide solutions to the implementation problems and present them organized according to GDPR principles and requirements. Some work has already been in progress to help companies with this matter, as presented in section 2 but most are tools or work done for specific cases. Privacy by design is also a domain that is very connected to the matter and already has many patterns, but they are not organized to help with the specific case of GDPR.

This document is structured in 5 sections. In the next section, some background and related work are described, including GDPR principles, Privacy by Design, Patterns, as well as existing tools and

practices for GDPR compliance. Section 3 shows the solution's proposal with an overview of it, followed by the definition of the solution's approach and the solution itself. Next, in chapter 4, a demonstration of how the library can be applied using a case study is presented. In the last section, we conclude and present the future work.

2 BACKGROUND AND RELATED WORK

2.1 GDPR

The General Data Protection Regulation (GDPR) is a standardized and enforceable law across all EU Member States (Moné, 2018), allowing citizens to understand "how" and "what for" their data is being used. In simple terms, this regulation applies to any person, the data subject, in the EU whose data is being processed by an organization (e.g., legal person, public authority, institute, etc.) that operates within the EU, whether the processing is done in or outside of the European Union (Art. 3 of GDPR).

The regulation has terms like Data Controller, which is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Art4, paragraph 8). Moreover, enforces Consent, "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Art4, paragraph 11).

2.1.1 GDPR Principles

The GDPR brings a set of principles that are related to the processing of personal data. EXIN, Verheijen (2017) resumes them in 6 principles, which we can find in Article 5 (Intersoft Consulting, 2020). These are the principle of purpose limitation (paragraph 1, sub b GDPR, Principle of data minimization (paragraph 1, sub c GDPR), the principle of trueness and accuracy (paragraph 1, sub d GDPR), the Principle of storage limitation (paragraph 1, sub e GDPR), and the Principle of integrity and confidentiality (paragraph 1, sub f GDPR).

The principles of lawfulness, fairness, and transparency (paragraph 1, sub a GDPR) are further explained in Articles 7, 8, 9 GDPR; the transparency part is in Art. 12.

Besides the ones resumed in EXIN, Verheijen (2017), Art. 5(2) also indicates the principle of accountability.

2.2.2 Rights of the Data Subject

In chapter 3 of the GDPR, the regulation describes the data subject's rights that controllers need to ensure to comply with the regulation. Articles 13 and 14 express what needs to be informed to the data subject when the data is collected. Article 22 discusses automated individual decision-making, and Article 22 the restrictions. For this work, we will focus on Articles 15 to 21.

The rights are: Right of access by the data subject (Art. 15), Right to rectification (Art. 16) refers to the right of data subject having their data accurate, allowing rectification of inaccurate data, Right to erasure ('right to be forgotten') (Art. 17), Right to restriction of processing (Art. 18), Notification obligation regarding rectification or erasure of personal data or restriction of processing (Art. 19), Right to data portability (Art. 20), and Right to object (Art. 21).

2.2 Privacy by Design

Privacy by Design is about considering privacy when designing systems and relates to GDPR Compliance because some of its principles are similar to the legislation's requirements. Verheijen (2017) in EXIN Privacy & Data Protection states that: "required level of data protection must already be taken into account at the design stage for the processing method".

2.2.1 Privacy by Design Principles

Cavoukian (2010) names the principles in the foundation of this approach which have several similarities to the GDPR principles.

- First – Proactive and Preventive
- Second – Privacy as the Default
- Third – Privacy embedded into Design
- Fourth – Full functionality (Positive-Sum)
- Fifth – End-to-end Security
- Sixth – Visibility and Transparency

2.2.2 Privacy by Design Strategies

Colesky et al. (2016) divides the requirements into strategies, which are "architectural goals in privacy by design to achieve a certain level of privacy protection". These goals are:

Minimize: limit the data to only the essential for our system, reducing the breach impact.

Hide: use of cryptography and restrict access to only authorized personnel, helping reduce the probability of a breach.

Separate: distributing or isolating storage also helps in reducing the probability of a breach.

Abstract: limit the detail of information, reducing the impact of a breach.

Inform: inform the data subject of changes, requests, retention of the data, and notify them when a breach occurs.

Control: the consent to, update and retract data from the data subject, control over their personal data.

Enforce: ensuring the commitment to the GDPR requirements, policies, and legislation by updating and chasing the wrong practices.

Demonstrate: having evidence of the compliance with GDPR by having logs and audits to extract better the goals and effects of the actions performed on personal data.

Table 1: Association of Hoepman's Privacy by Design Strategies and GDPR Principles.

Strategies \ GDPR Principles	Purpose Limitation	Data Minimizations	Trueness, Accuracy	Storage Limitation	Integrity and Confidentiality	Lawfulness	Fairness	Transparency	Accountability
Minimize	x	x							
Hide				x	x				
Separate					x				
Abstract				x					
Inform			x					x	
Control						x	x	x	
Enforce									
Demonstrate									x

In Table 1, we can see how the GDPR principles and Hoepman's Privacy by Design strategies can be associated.

When designing the systems, it is necessary to keep in mind these requirements and principles to achieve

2.3 Patterns

As mentioned in the introduction, patterns are used to solve recurrent problems in an outlined way we can use patterns. There are and have many domains to which they can be applied, has Privacy by Design; to better comprehend this topic, previous works and studies were analyzed.

In Doty & Gupta (2013), three sample patterns are provided from *privacypatterns.org*. One of them has a strong correlation to GDPR compliance; Location granularity: Collecting more information than needed can harm the user's privacy and increase the risk for the service (in the case of a security breach, for example), but the location data may still need to be collected to provide the service[1]. The other two, Asynchronous notice and Privacy Dashboard, at a first read, may not appear to be relevant to GDPR compliance, but they do, and in fact, they are used in the library.

This project's (*privacypatterns.org*) goal is "for this to be a living document constructed by the community of engineers, designers, lawyers and regulators involved in this topic"[2]. So, since the publication of Doty & Gupta (2013), more patterns were added. In this website, the patterns are divided by Privacy by Design strategies and are generally defined by Summary, Context, Problem, Solution, and Consequences. This library is very relevant to the solution we are proposing.

In 2017, a literature study was conducted on privacy patterns; in this research, the authors found a lack of studies focused on pattern catalogs since some were quite specialized (Lenhard et al., 2017). In the study, the authors state that "the published research results show a clear focus on the privacy design strategies of hide and separate" (Lenhard et al., 2017). No patterns were provided in Lenhard et al. (2017) since the goal was to characterize and classify the different researches on this topic.

2.4 Existing tools and practices for GDPR compliance

With the emergence of the regulation, many companies started to provide frameworks, like LeanIX (2020), a framework that helps the companies in categorizing data objects in terms of privacy sensitivity, identifying responsibilities, classify the data in heatmaps, and many other concerns. However, it does not show what is needed in terms of enterprise architecture. Instead, it does that job for the user.

The PDP4E (2020) is a project that aims to "widespread the creation of products, systems and services that better protect the privacy and personal data of EU citizen". PDP4E presents some papers and have participated in conferences about risk management[3], privacy-aware design[4], and other topics. The PDP4E project focuses more on tools and GDPR/privacy awareness, so no specific solution is provided.

A practical and design-oriented approach in order to solve GDPR's requirements is provided in Hjerppe

[1] https://privacypatterns.org/patterns/Location-granularity
[2] https://privacypatterns.org/about/
[3] https://www.pdp4e-project.eu/risk-management/
[4] https://www.pdp4e-project.eu/privacy-aware-design/

et al. (2019). The article divides the requirements and principles mentioned above into nine requirements that a system should take into account in its architecture: system security and privacy, data minimization, consent control, data traceability, user access, data rectification, data erasure, data restrictions, and data's physical location. This work provides what requirements need to be in mind and some architectural solutions (like logs), but it does not provide patterns.

Rösch et al. (2019) provides patterns (technical solutions) for some of the GDPR principles (or requirements as definied in the paper) and data subject's rights. This paper is very relevant to this research but lacks modeling, and it is incomplete, as they mention in the paper; so, these patterns will be kept in mind for the solution but do not satisfy what is needed.

A BPMN proposal for a better understanding of the requirements brought in with the GDPR is created in Calabró et al. (2019). The authors' approach involves defining a use case (a simple BPMN), gather authorization requirements, business requirements, and security best practices. Then an identification of the business process affected by the GDPR requirements is performed, and the statements are transformed into machine-interpretable language. The final steps are the test of the architecture, its deployment, the policies, and, at last, an access review. Nevertheless, they present are no patterns.

Palmér (2017) proposes an architectural meta-model for the EU Directive (Directive 2016/680). It is a directive concerned with the protection of people regarding the processing of data, created in April of 2016. Although both regulations concern processing data, they are not the same, so it has some differences in requirements and constraints. The work presents models in ArchiMate, but some mismatch occurs because it follows the EU Directive 2016/680 and not with the General Data Protection Regulation; also, a map of the architecture is modeled and not a pattern.

Some researches lack modeling, while others lack a more pattern-oriented approach, and some others are incomplete; nevertheless, all the learnings acquired when assessing these documents were considered when proposing and creating the final solution. The goal of this work is to create a library that guides companies and provides solutions in order for them to achieve GDPR compliance, so patterns from privacypatterns.org (the website referenced in Doty & Gupta (2013)) and from Rösch et al. (2019) were considered to be part of the library.

3 BUILDING AND ORGANIZING PATTERNS FOR GDPR COMPLIANCE

3.1 Solution Overview

As presented previously, there are already patterns in the Privacy by Design domain. However, a collection of patterns organized in terms of the General Data Protection Regulation principles and the data subject's rights intertwined does not exist.

Another particularity of the proposed solution is the definition of use cases. This approach is expected to make it easier to search and find which patterns make sense for each case (since not all the patterns need to be applied to all projects). Also, we based most of the use cases on the data subject's rights, providing a connection between these rights and the principles relating to the processing of personal data.

The proposed solution starts by **identifying the entities** (stakeholders and objects), then proceeds to **define the use cases** by analyzing the business processes needed, select the GDPR principles associated and the entities present, and later, if possible, model them.

For each use case and its principles, **relevant patterns are retrieved** from sources privacypatterns.org and Rösch et al. (2019) and adapted to our template. We will then **check** if all the use cases have at least one pattern associated, and if not, we create or adapt a pattern for it.

After creating a GDPR pattern library, we **verify** if the patterns are relevant and applicable to a Case Study. After the application of the patterns, the last step is their **evaluation**.

3.2 Entities and Use Cases

To better organize the library, use cases were defined, and the entities present were selected

The entities identified are the data subject (who can be a child), the data controller, the data processor, third-party, and data subject's holder of parental responsibility, that for the rest of the paper will be expressed as guardian (or guardian of the minor).

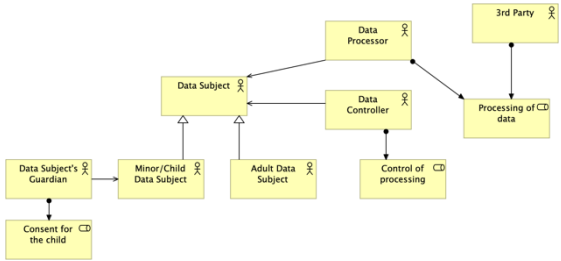

Figure 1: Entities and their relations

Since most of the use cases are related to the data subject's rights, we can presume that the data subject will be present in almost all the use cases. This happens because of requests performed by the data subject itself, as the request for erasure, or because of controller's requests, like the request for consent.

The data subject is the holder of personal data that can be identified by reference to that personal data. However, in this library, the data subject will only be the client/user of the organizations' services.

It is also relevant to point out the difference between controller and processor since they are related. As explained in section 2.1, a controller is a person with legal authority that determines the purposes and means of personal data processing. A processor is a person who processes ("any operation or set of operations which is performed on personal data or on sets of personal data") the personal data on behalf of the controller. All these definitions are explained in depth in Article 4 of the regulation.

A third-party is an entity that is not a data subject, a controller, or a processor authorized to process personal data. It can even be from another country or even from outside of the European Union (EU).

All the entities related to a "minor" are for a child that, according to the regulation, is a data subject below the age of 16 years old, but the Member States can change it (although the age cannot go below 13 years) Art. 8. In Figure 1we can see the relations between the entities and some of their roles.

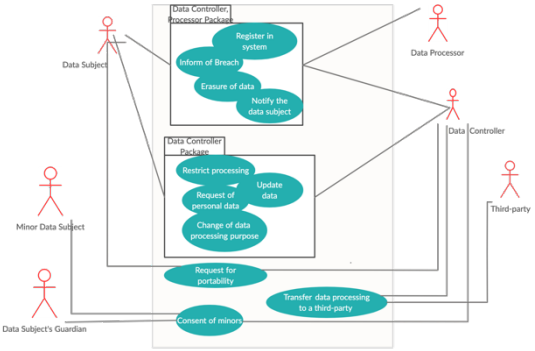

Figure 2: Use Cases

Figure 2 is a UML Use Case diagram with all the use cases. The use cases with the same entities are grouped in packages for a clearer view.

Before declaring the use cases, an explanation of their use is necessary. The use cases work as a way to organize the library per se and organize it in terms of the GDPR. The use cases are mostly situations that come from the rights of the data subject, and in each use case, we also have the general principles that govern data processing.

The first use case is Register in system. It concerns all the constraints organizations need to be aware of when collecting data in registration.

Inform of a breach is a use case that is probably already addressed by many organizations. However, the GDPR brings some requirements that probably were not contemplated before, like the controller notifying the supervisory authority of the breach within 72 hours and, if necessary, inform the data subject; it also has to follow the guidelines present in Article 33(3).

The next use cases are particular to the regulation, mostly with the data subject's rights, and are related to requests.

Request for restriction on personal data's processing focuses on the right to restrict the processing that is being performed.

The other request is when the data subject asks for the data being processed and other information stated in Art. 15(1). It is called Request of personal data.

The Request for portability concerns the right to request the data from the data controller in "a commonly used and machine-readable way" (Art. 20 of GDPR). They can also transfer it to another controller or request the data to be directly transmitted, if possible.

The most commonly known might be the Request for erasure, also known as "the right to be forgotten.

Finally, in terms of use cases related to the data subject's rights, we have the Request for or the ability to update their personal data. The data subject must be able to access their data quickly and update it.

Another use case contemplates when new policies or purposes appear in the data processing; this is called Change of Processing Purpose.

Regarding Consent of minors, as mentioned in the entities, a minor, in the regulation, a child younger than 16 years old, cannot consent for the processing; the same has to be given by a guardian, the holder of parental responsibility over the child.

Many companies subcontract others to process the data they collected, in or outside of the country or EU; so, a use case regarding Transfer data processing to a third-party is relevant.

Lastly, we have a use case present in others, but since it is very relevant and can be used for other cases, it is on its own; this is the use case Notify the data subject.

The use cases were selected considering the broadest concerns and requirements of the regulation; more specific or industry-specific use cases are not addressed in this research.

3.3 Template for Patterns

One of the characteristics of patterns is their template, an explanation of what problem it addresses, and the proposed solution.

In this research, the template created has the base elements, Context, Problem, and Solution and elements present on the website. The pattern template proposed considers what and how the pattern addresses the problem and the use cases for the search in the library.

The template for the patterns has the following fields:

Associated Use Case: The use case in which the pattern is applicable and a brief description of it (with a model of some of the general processes necessary).

Associated GDPR principles: The GDPR principles that the patterns aim to solve.

Name: Name of the pattern.

Context: The situation where the pattern may be applied.

Problem: The problem the pattern addresses.

Solution: The solution principle underlining the pattern.

Source: If the pattern exists in the accessible libraries, the source is included.

A simple diagram of the pattern is also present in the library to give a general idea of the pattern's solutions and requirements.

In the template, we see that, for each use case, GDPR principles are associated; this helps to see the main concerns to the problem, but it also helped in the search for the patterns. As was shown in Table 1, the principles are related to different Hoepman's Privacy by Design strategies; since these patterns are in the Privacy by Design domain, the strategies are some of the categories through which the search is done. However, not all the patterns for Privacy by Design are related to the GDPR, since the concern for privacy in the early stages of a "project" is prior to the creation of the regulation, and there are more problems related to privacy than the ones the GDPR brings. Some of the problems that patterns address are for specific cases, like mobile applications, so a thorough and careful search was performed to find patterns that focused on more broad scenarios.

In each use case, the models provide an overview of the constraints and requirements that come with the GDPR and show some of the "sub-processes" needed to take into account. A model of the pattern is relevant; although not all solutions have architectural bases, a simple and image type of view helps to see what is needed to be implemented clearly. A brief explanation of what it is and what articles in the GDPR are related to the problems that need to be addressed is also contemplated. This way, any person can analyze the regulation if they have a specific concern that is not covered in the library already with an idea of what to search for, making the search quicker.

A use case does not address only one principle, consequently, doesn't have only one problem associated with it, so the context of the pattern is important to see each situation (or process in the use case) we may apply the pattern. The problem and the solution are essentials for this type of library.

3.4 Retrieval of Patterns

When it came to retrieving patterns from the sources, not all use cases had the same ease. In this section, the list of the patterns will be presented, but first, some of the difficulties that came with the retrieval of patterns will be assessed.

One of the terms/concerns in the GDPR is Consent, and probably because it was the most visible change that companies and organizations had to comply to and it was already a known concept from its predecessor (i.e., Directive 95/46), a variety of patterns were found in this category. Not all could be used in the library because they are focused on particular cases, like the one presented above: Location granularity, which only focuses on the data subject's location-related data. Notification is also vastly addressed, but for many specific cases like pop-up notifications or icons for mobile applications.

In contrast, patterns related to the data subject's rights were trickier to find since it is not a visible change, and many users may not be fully aware of its existence. For example, we found patterns that some companies have already used for the data subject requesting their data. For the case of portability, it was harder to find patterns that addressed this matter, specifically when controllers provide the data directly to other controllers by the request of the data subject. This was solved using other use case patterns but adding a process of requesting to whom and how to send the information.

The erasure request also does not have many patterns. Although it may seem simple to erase data from a database, the GDPR also requests additional information to be stored and saved that has to be eliminated as well.

The concerns related to processing minors' personal data were also not easy to find; not only the child's age must be known, but the guardian also has to be aware of the processing and give consent. In this case, the controller has to decide if minors will use the service or not because if they will, age has to be a requested data. If not, it may not be relevant to process the data subject's age.

Here is the list of all the patterns and their use cases, accompanied by a brief explanation of what they address:

Table 2: Selected Patterns.

Use Case	Patterns	Brief Explanation
Register in system	Minimal Information Asymmetry	The first two patterns are related to purpose limitation, and data minimization, the next four are about integrity and confidentiality and the last three are about consent.
	Awareness Feed	
	Encryption with user-managed keys	
	Aggregation Gateway	
	User data confinement pattern	
	Personal Data Store	
	Lawful Consent	
	Informed Implicit Consent	
	Obtaining Explicit Consent	
Inform of Breach	Data Breach Notification Pattern	The first pattern focuses on quickly detecting and reacting to data breaches, and the second one is more related to authentication.
	Unusual Activities	
Request for restriction on personal data's processing	Negotiation of Privacy Policy	These patterns are about a data subject negotiating and being able to push and pull data for processing.
	Reasonable Level of Control	
Request of personal data	Personal Data Table	These patterns give the data subject the ability to see the data and logs and transfer the data to their computer.
	Privacy Dashboard	
Request for portability	Personal Data Table (adapted)	These patterns are primarily for portability for the data subject, so the possibility of sending directly to another party can be added.
Request for erasure of data	Technical Solution for Right of Erasure	This pattern states what the services must have to provide a simple way of processing the request of erasure of data.
Request for/and update of data	Technical Solution for Update of data	This pattern is a simple solution for what is needed for the data subject to see their data and update any mistakes or changes.
Change of data processing purpose	Negotiation of Privacy Policy	This pattern is already used for another use case but is also relevant because of the opt-in/opt-out options since new purposes can be added and request for new consents.
Consent of minors	Lawful Consent (adapted)	The idea is to adapt the lawful consent pattern but use the guardian of the child for consenting.
Transfer data processing to a third-party	Sticky Policies / Obligation Management	The patterns focus on building trust and assuring that the third-party follow the GDPR.
	Trust Evaluation of Services Sides	
Notify the data subject	Asynchronous notice	One pattern covers possible breaches, and the other covers more general matters.
	Unusual Activities	

3.5 Example of Library

Since the library is extensive, it is impracticable to present it all in this paper. We selected two patterns, Technical Solution for Right of Erasure and Sticky Policies from different use cases to show the patterns in the designed template.

The first one is related to case of erasure of data and it was adapted to this library.

Associated Use Case: Request for erasure of data

The data subject has the right to have the data concerning him/her erased if the terms in Art 17(1) are met without unjustified delays. The controller or processor has to ensure that all the data is deleted, while taking into account the available technology and the cost of implementation, and he must inform the processors of what was requested to be erased.

The entities present in this use case are:

• Data Subject (Client)

• Data Controller

Associated GDPR requirements:

• Purpose limitation

• Principles of lawfulness, fairness and transparency

• Data subject's right to erasure or "right to be forgotten".

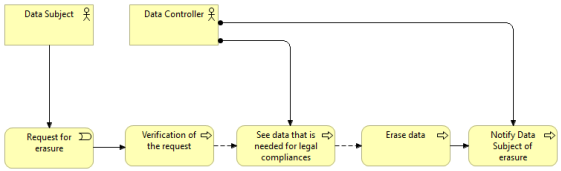

Figure 3: Model of Request for erasure of data use case

Name: Technical Solution for Right of Erasure

Context: Services that process personal data want their users to trust in them and comply with the new regulations. In some cases, the users do not want to use the services anymore or may want their data to be removed from the service database for various reasons.

Problem: Since the appearance of the GDPR, many users are familiar with the right to be forgotten but may not know precisely when to use it. The controller then has to make sure that the request is liable and that if some unlawful processing is occurring, it should be addressed and resolved. It is also vital that the data needed for legal concerns cannot be deleted. The user needs to be made aware of these situations to be transparent (a store cannot delete the registry of a purchase because of financial constraints).

A controller may not want the users to withdraw their data, but it is crucial to guarantee the user that their rights are being fulfilled and increase the trust with the user.

Forces and Concerns:

- Users want to have the possibility to have their data removed not only from processing but also from the services database entirely.
- Users may not fully understand in what terms they can request for the erasure of their data.
- Controllers want to ensure the users trust in their service.
- Controllers need to check if the data has reasonable reasons for its erasure.
- Controllers must verify if the data is required for legal claims and if so, they need to notify the user about it.

Solution: The first step to take is to create an interface that enables personal data's subsequent erasure. Data of individual persons must be retrievable and separately erasable. Subsequent reproduction of the data after deletion is not permitted.

After the data subject requests for the erasure of their data, the controller must assure that the request has the right grounds for the erasure to be conducted. If one of the grounds is met, then the controller must check if some of the data needs to be kept to comply with legal obligations. When all of the erasure requirements are met, the data then has to be tracked and deleted from the services database, as well as the logs related to the data subject in question, them a notification of the deletion is sent.

When no ground is encountered or other obligations require the data to be kept, the data subject should be notified of the matter.

Source: adapted from Privacy Control Patterns for Compliant Application of GDPR (Rösch et al., 2019).

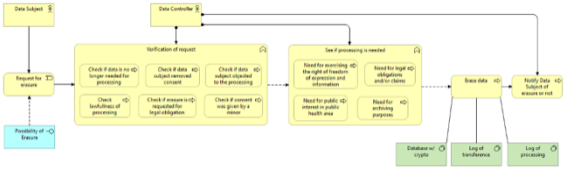

Figure 4: Model of Technical Solution for Right of Erasure

The second pattern is related to transferring the processing to a third-party and how to provide organization's information for lawful processing.

Associated Use Case: Transfer data processing to a third-party.

In some cases (like subcontracts), the processor or controller share the data with a third-party. When this happens, the data subject must be notified of such actions. For this transfer to be valid, the Commission has to decide that the third-party is trustworthy, i.e., follows the processing policies/ restrictions present in the GDPR legislation. In the absence of a decision by the Commission, the transfer may also be made if "the controller or processor has provided appropriate safeguards" (Art.46) or the data subject has to consent to the processing being aware of all the risks (Art.49). According to article 19, "any rectification or erasure of personal data or restriction of processing" must be notified to whom the data was transferred. It is also important to point out that this is referent to other

companies in the same country and a third country or an international organization (Chapter 5, Art. 44-50).

The entities present in this use case are:

- Data Controller
- Third-party

Associated GDPR principles:

- We come across all of the GDPR principles (since all the regulation must be followed)
- Accountability

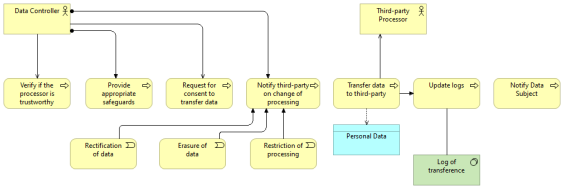

Figure 5: Model of Transfer data processing to a third-party use case

Name: Sticky Policies or Obligation Management

Context: Multiple parties are aware of and act according to a certain policy when privacy-sensitive data is passed along the multiple successive parties storing, processing and sharing that data.

Problem: Data may be accessed or handled by multiple parties that share data with an organisation in ways that may not be approved by the data subject.

Solution: Service providers use an obligation management system. Obligation management handles information lifecycle management based on individual preferences and organisational policies. The obligation management system manipulates data over time, ensuring data minimization, deletion and notifications to data subjects.

The goal of the pattern is to enable users to allow users to control access to their personal information. Examples of policy specification languages include EPAL, OASIS XACML and W3C P3P. Tracing of services can use Identifier-Based Encryption and trusted technologies.

Source: https://privacypatterns.org/patterns/Sticky-policy
https://privacypatterns.org/patterns/Obligation-management

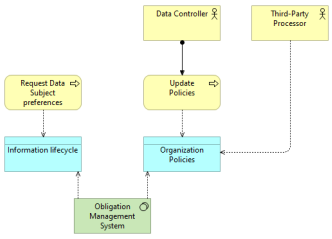

Figure 6: Model of Sticky Policies or Obligation Management

4 CASE STUDY AND DISCUSSION

This library's central goal is to help companies better understand how the GDPR affects the design of their services and what are some of the solutions for it.

For demonstration purposes, consider a platform that provides some news to the client. The client must register in the platform, so the patterns for the use case regarding registration can be used, not just the ones related to consent. The system needs to ensure that the retrieved data is only the essential one; for example, if the news only comes through email, a phone number does not need to be collected. A relevant pattern is Minimal Information Asymmetry.

For this kind of service, not all the patterns are relevant, but that is the benefit of this library's organization. Since minors probably will not use this service and the processing of data is internal to the company, the use cases related to these matters can be ignored, so the search for patterns to use becomes quicker. Also, since the idea of patterns is to provide a solution that can be used multiple times in different ways, the company can adapt them to the platform and re-use them for other services. If the platform changes or new information is provided for some reason, the use case for a change of purpose and its patterns becomes essential.

In terms of storage, the patterns provide different solutions, and so the controller and the processor must discuss which ones apply. The patterns focus more on processing the data and having access to it without being entirely responsible for storing it internally. These may be more suitable for smaller companies or ones that do not need that much information (as in this example).

An ArchiMate diagram presents some of the changes the patterns brought in the case study described.

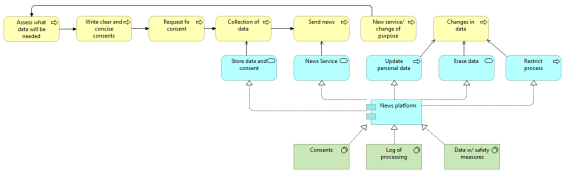

Figure 7: Simple model of the case study after the application of the patterns

In Figure 7,we can see the presence of logs and the consents' storage to which the data subject agreed. This storage is not present in many services since consent is not the only way to have lawful data processing. The pattern Minimal Information Asymmetry requires new business processes. The

careful analysis of what data is strictly necessary for the service, the writing of concise and straightforward consent to each purpose, and considering the data subject's comprehension for what their data will be used are some of the processes necessary to comply with the GDPR. Also, application services for compliance with the data subject rights are required and essential.

This case study demonstrated how the proposed library is helpful in the context of GDPR compliance.

It is easier to implement design modifications in new projects, but these patterns may be used for already working services. The diagrams support the description of the use cases and solutions, making it easier to understand what needs to be implemented and added to ensure GDPR compliance..

5 CONCLUSIONS

Data protection is important and crucial in a business, especially when personal data is stored and processed. The creation of GDPR confirms it. In an era where our data is easily acquired and processed without the owners' knowledge and sometimes without their consent, the regulation gives guidelines and rules for the organizations that operate in the EU to follow. The challenge is that there is much information and constraints to follow, and the language is not very explicit nor give objective rules to follow. This research contributes to ensuring Information Systems compliance to the GDPR, presenting ways of achieving it, using a library of patterns. When creating this library, the description and modeling of the use cases were performed, and the definition of the associated entities and GDPR principles. A search through the sources was conducted to select the patterns that better solve the problems that the GDPR requirements bring to the use cases, and when needed, new patterns were created. In total, 22 patterns compose the library. This collection of patterns is used in the case study, demonstrating how services that require personal data processing may use the proposed solution and what changes when the patterns are applied. Although very important in the design phase of a project, these concerns are permanent throughout its lifecycle. To point out that data processing occurs not only for users but also for the company's employees.

In the future, we expect to add other patterns to the library, especially to the use cases where the patterns were hard to retrieve. Additionally, an interface could be created to show the collection of the use cases and patterns in a more dynamic way. Another future path to explore is developing a library that is focused on use cases for inner-company problems since the employees are also data subjects. With this, other concerns appear since the processing of personal data may not require consent due to contractual reasons.

REFERENCES

Intersoft Consulting, n.d. *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/. Last accessed in 24.11.2020

Alexander, C., Ishikawa, S., Silverstein, M., 1977. *A Pattern Language: Towns, Buildings, Construction,* Oxford University Press.

Moné, L., 2018. How to Solve GDPR with Enterprise Architecture: A Case Study, *LeanIX*. https://www.leanix.net/en/blog/how-to-solve-gdpr-with-enterprise-architecture Last accessed in 24.11.2020

Verheijen, R., 2017. *EXIN: Privacy & Data Protection, Whitepaper: Data Protection: Compliance is a Top - Level Sport*, EXIN and Secura.

Cavoukian, A., 2010. *Privacy by Design The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices*. Ontario, Canada.

Colesky, M., Hoepman, J., Hillen, C., 2016 A Critical Analysis of Privacy Design Strategies. In *2016 IEEE Security and Privacy Workshops (SPW)*, San Jose, CA.

Doty, N., Gupta, M., 2013. *Privacy Design Patterns and Anti-Patterns*. UC Berkeley, School of Information. California.

Lenhard, J., Fritsch, L., Herol, S., 2017. A Literature Study on Privacy Patterns Research. In *2017 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. Vienna.

LeanIX GmbH, n.d.. *Mastering the GDPR with Enterprise Architecture,* LeanIX. Bonn, Germany.

PDP4E Project, n.d.. *PDP4E.* https://www.pdp4e-project.eu/ Last accessed in 24.11.2020

Hjerppe, K., Ruohonen, J., Leppänen, V., 2019. "The General Data Protection Regulation: Requirements, Architectures, and Constraints". In *2019 IEEE 27th International Requirements Engineering Conference (RE)*. Jeju Island, Korea (South).

Rösch, D., Schuster, T., Waidelich, L., Alpers, S., 2019. Privacy Control Patterns for Compliant Application of GDPR. In *25th Americas Conference on Information Systems*. Cancun.

Calabró, A., Daoudagh, S., Marchetti, E., 2019. Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study. *ITASEC*. Pisa, Italy.

Palmér, C., 2017. *Modelling EU DIRECTIVE 2016/680 using Enterprise Architecture*, KTH, School of Electrica l Engineering (EES). Stockholm, Sverige.