Towards Designing a Privacy-Oriented Architecture for Managing Personal Identifiable Information

Adán F. Guzmán-Castillo[1], Gabriela Suntaxi[2]*, Bryan N. Flores-Sarango[3] and Denys A. Flores[4]

[1]Department of Informatics and Computer Science, Escuela Politécnica Nacional, Quito, Ecuador.
adan.guzman@epn.edu.ec, https://orcid.org/0000-0003-4763-8506

[2*]Department of Informatics and Computer Science, Escuela Politécnica Nacional, Quito, Ecuador.
gabriela.suntaxi@epn.edu.ec, https://orcid.org/0000-0002-0298-5144

[3]Department of Informatics and Computer Science, Escuela Politécnica Nacional, Quito, Ecuador.
bryan.florers04@epn.edu.ec, https://orcid.org/0009-0007-7030-8501

[4]Department of Informatics and Computer Science, Escuela Politécnica Nacional, Quito, Ecuador.
denys.flores@epn.edu.ec, https://orcid.org/0000-0002-5068-1559

Received: October 07, 2023; Accepted: December 15, 2023; Published: February 29, 2024

Abstract

Recent threat reports have warned researchers and security professionals about a shortage of cybersecurity skills to face devastating personal data breaches. As a response, governments have taken on the challenge of proposing specific legislation to protect citizens' privacy while holding information-processing companies accountable for any misuse. However, unauthorized access to such information, or possible negligent destruction of personal records are some issues that cannot be dealt with privacy laws alone. In this research, we introduce the functional requirements to deploy PriVARq, a novel privacy-oriented architecture to proactively manage any consensual submission of personal identifiable information (PII); i.e. during its collection, processing, verification and transference. PriVARq's main contribution is the balance between legal frameworks and industry-leading security standards to mitigate the former's shortage of practical solutions to tackle some privacy and security issues when dealing with PII. Consequently, for defining PriVARq's functional requirements, a privacy-by-design approach is employed which not only considers legislation proposed in Europe and Latin America but also analyzes technical aspects outlined in international security standards. We aim to provide a proactive approach to reduce the shortage of skills and solutions to tackle privacy leakages in public repositories and devise future research venues to implement PriVARq in public and private organizations.

Keywords: Privacy, Architecture, Personal Data Protection, Data Privacy, PII, Personal Identifiable Information, Requirements, GDPR, LOPDP, ISO 27001, NIST SP 800-53, Privacy-by-design Techniques.

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 1 (February), pp. 64-84.
DOI: *10.58346/JISIS.2024.I1.005*

*Corresponding author: Department of Informatics and Computer Science, Escuela Politécnica Nacional, Quito, Ecuador.

1 Introduction

Recent security reports (Fortinet, 2022; Ariganello, 2022; EC-Council, 2022; Luxon, 2021) warned us about an increasing lack of threat intelligence inside organizations. For instance, the Fortinet Cybersecurity-Skill Gap Report analyzed the experiences of companies in 29 countries (Fortinet, 2022). Here, inherent readiness deficiencies were revealed which pose security and privacy challenges against personal identifiable information (PII) in the near future. Particularly, 87 percent of Latin-American companies revealed having faced at least one security breach in the last 12 months, with more than 5 breaches reported in at least 17 percent of them. Although most of the consulted CEOs acknowledged the increasing cybersecurity risk in their companies, 64 percent of them reported costs of security breaches to be equal to or greater than USD $1 million, evidencing a severe lack of commitment to overcome these challenges. In fact, some security threats to PII, such as authorization creep, credential misuse, and data manipulation/destruction/disclosure, are caused by either the lack of third-party access control or privileged insider misuse. Then, if any security incident arises during the collection, processing, verification, and transference of PII, privacy issues might also affect its owner's rights.

Consequently, legal instruments have been proposed worldwide to counter these problems. For instance, the Ecuadorian Organic Law of Personal Data Protection (LOPDP) (Registro Oficial Ecuador, 2021), and the European General Data Protection Regulation (GDPR) (European Union, 2019) are proposed to protect the privacy of data owners, i.e., the citizens. Furthermore, since privacy issues are generally collateral damage of security incidents, there are also security guidelines to protect the confidentiality, integrity, and availability of information (whether personal or not), such as the information security standards proposed by both the ISO and the NIST. However, even with privacy laws and security standards, there is no straightforward way to implement them within a secure computer architecture due to the lack of specific technical guidelines.

Although the enforcement of privacy regulations started earlier in European countries than in Latin American countries, from their experience, studies have demonstrated that privacy compliance is not a trivial task, which calls for a structured approach to manage and understand privacy requirements and implementation techniques (Mikkonen, 2014). Actually, recent surveys within small-to-medium organizations reported several challenges in understanding compliance with privacy-focused legal instruments and how to implement their requirements to protect PII (Sirus, Nurse, & Webb, 2018).

In this research, we fill this gap by defining the actors, requirements, and techniques to deploy PriVARq, a novel privacy-oriented architecture to aid the secure collection, processing, verification, and transference of PII, i.e., managing the overall PII's life cycle. For better understanding, in our current work, design details and operational components of PriVARq are given, avoiding complex technical details for its implementation. The rest of the paper is organized as follows: In Section 2, related work in the field of PII protection is presented. In Section 3, we analyze recent data protection legislation, security standards, and privacy-by-design techniques to define PriVARq's actors and requirements. Next, Section 4 explains the methodology used for mapping such actors and requirements with privacy-by-design techniques. Then, in Section 5, PriVARq’s design is introduced, considering actors, requirements, and techniques to deploy each component. Finally, conclusions and future work are presented in Section 6.

2 Related Work

In this section, we discuss some related work about different architectures for data protection. An architecture was proposed for PII storage based on Ethereum and IPFS (Alessi et al., 2018). It uses a mobile application to read, modify and share PII with external services that make an explicit request. This solution extends the Personal Data Store (PDS) concept by using a dedicated ontology and a distributed architecture leveraging a particular profile schema. On the other hand, although an SDN-based architecture was proposed (Ujcich and Sanders, 2019) to prevent data protection breaches by identifying data protection intents using some regulatory requirements outlined in the GDPR, it could not verify privacy compliance in record keeping. Conversely, an interesting personal health record exchange scheme based on blockchain was proposed (Wang et al., 2019). Here, the patient manages and distributes the private attribute key to the user, allowing a decentralized fine-grained access control without relying on third parties. Despite being convenient and fast for integrity checks of health records using smart contracts, it relies heavily on the patient's trust, which may be counterproductive for key revocation if the number of users increases. A similar work was proposed in which the authors aim to solve the trust problem in health record sharing (Hernandez et al., 2021). Here, a knowledge dataspace defines data permissions and access concessions to increase user trust. This solution provides a highly trusted environment for PII management, access control, and data privacy.

In summary, the technical requirements for data protection identified in these works are not exhaustive despite being closely related to the GDPR. Also, such requirements may only be applied to healthcare information systems but could not generalize well to other applications and needs for PII collection, processing, verification, and transference. Also, since some security aspects are generally overlooked in legal-based solutions, in this article, we redefine functional requirements for privacy preserving solutions so that technical aspects and legal compliance can be balanced and applied to other problems. In fact, to avoid privacy issues derived from the insecure behavior of computer systems, with PriVARq, we take a deductive approach in which privacy protection laws, security standards, and privacy-by-design techniques are analyzed prior to defining the architecture's operating requirements (Megias and Mazurczyk, et al., 2022).

3 Background

This section discusses the theoretical background on which our research is based.

3.1. Personal Data Protection Legislation

The General Data Protection Regulation (GDPR) is a widely known legal framework issued by the European Union (European Union, 2019) with increasing worldwide interest and implications (Goddard, 2017). Its main objective is to protect PII and how organizations process, store and dispose of such information. This law controls organizations that may use personal information by enforcing stringent rules to prevent unauthorized access and violation of personal rights. Like the GDPR, in Latin America, several countries have adopted similar legislation (Alimonti and Rodríguez, 2020).

Chile was the first country in the region to enact a Law for the Protection of Private Life in 1999 (Herrera Carpintero, 2016). By 2000, Argentina implemented the Personal Data Protection Act to enable the international transfer of PII with the European Union (European Union, 2003). Later in 2011, Peru issued the Law for Protection of Personal Data, which led the initiatives to secure personal

information from unauthorized access (Angarita, 2012). On the other hand, Uruguay issued the Law No. 18, 331 about Personal Data Protection and Habeas Data Action, which allowed this country to be declared appropriate for transferring personal information with the European Union (Angarita, 2012). As for Brazil, it was the first Latin-American country to develop a Personal Data Protection Law based on the GDPR, which was published in 2018 (Ministerio da Cidadania Brasil, 2018). Similarly, the Organic Law for Personal Data Protection (LOPDP) (Registro Oficial Ecuador, 2021) was published in Ecuador on May 2021 to regulate the legitimate treatment of citizens' PII. With this law, each Ecuadorian organization that collects and processes PII must implement tools, methodologies, and even architectures to guarantee its protection. To sum up, despite the existence of privacy laws in many countries, efforts fall short to implement them in the technological field because of the need for more research to enforce PII protection. Nonetheless, besides being an "organic or foundation law", the Ecuadorian LOPDP seems more GDPR-compatible, making it more relevant for our research since the other Latin-American laws need to be upgraded to be fully aligned with the current European GDPR (UASB, 2022).

3.2. Information Security Standards

The International Organization for Standardization (ISO) publishes the ISO/IEC 2700n standards for the effective implementation of information security management systems (ISMSs) within organizations (ESGInnova, 2022a). The requirements outlined in the ISO 27001 standard provide security controls to protect information from security threats while preserving its confidentiality, integrity, and availability (ISO/IEC, 2020). Furthermore, the ISO 27002 standard establishes guidelines and general principles to initiate, implement, maintain and improve ISMSs within an organization (ESGInnova, 2022b). Both standards are essential for selecting, implementing, administering, and monitoring security controls to reduce any organization's information security risk.

In contrast, the National Institute of Standards and Technology (NIST) is an American agency created to promote technology standards for enhancing industrial innovation and competitiveness, including those related to computer security. For instance, in the context of our research, we use the NIST Special Publication 800-53 (Pillitteri, 2022) as it provides a security & privacy control catalog to protect information systems and their operations from various threats. These controls are flexible and customizable so they can be implemented as part of a corporate risk management approach.

3.3. Privacy-by-Design Approaches

It has been argued (Cohen, 2000) that any privacy legislation (such as GDPR) will face a problem related to privacy rights between individuals (holders of information), governments (political actors) and processors (technical actors). As a result, Privacy-by-Design (PbD) was introduced as a paradigm to examine potential data protection issues while designing or introducing a new technology (Schaar, 2010). PbD aims to avoid privacy allocation issues by considering protection requirements in the general computer system design prior its implementation. Therefore, any privacy protecting/defending architecture should be focused on balancing power between holders and actors while delivering conditions to guarantee accountability and transparency when handling private information. In this sense, PbD covers theoretical approaches and technical mechanisms for protecting privacy when individuals disclose information through a computer system.

Among such theoretical approaches, LINDDUN (DistriNet, 2020) and LINDDUN Go (Wuyts et al., 2020) have been introduced as privacy engineering methods based on threat modelling to ease the early identification and mitigation of privacy threats in software systems. These proposals consider PbD features that have been rather absent when defining models, processes and tools in the software development lifecycle (SDLC) to make it fully compliant with GDPR and similar legislations (Andrade et al., 2023). For instance, a human-centered approach has been proposed (Teresa Baldassarre et al., 2021) to enhance SCRUM so that privacy and security features can be introduced in agile software development. Similarly, the Unified Modelling Language (UML) has been refined (Alshammari and Simpson, 2018) to enable the abstraction of privacy principles during the software requirements elicitation phase.

Regarding technical mechanisms, computing architectures such as the EU DEFeND Project (Piras et al., 2019) have been proposed in order to support organizations in achieving GDPR compliance. However, such generalist approaches require developing auditing and government-managed controls to reduce the risk of data disclosure when specific operating features of PbD-based architectures are considered since early stages of their development.

Concluding, PbD approaches must consider privacy operating features within computer systems as a whole (holders, actors, processes, hardware and software) because privacy risks are directly associated to the level of data exposure (Morris and Lessio, 2018; Toch et al., 2018). Otherwise the inherent risk of privacy breaches may allow attackers to identify users depending on the granularity level of the information available for public mining. This is a problem particularly dangerous in cyber-physical systems where solutions are being implemented to mitigate security risks. For example, a blockchain solution has been proposed to provide access control in IoT devices and its data (Dorri et al., 2017). Likewise, differential privacy has been applied to prevent privacy breaches by using fog-computing based nodes to prevent user inference (i.e. PII) from data generated in smart meters (Cao et al., 2019).

4 Methodology

For balancing technical aspects and legal compliance, actors and requirements were mapped in Subsection 4.1, considering both the GDPR and the LOPDP, as well as the ISO 27001 and the NIST SP 800-53 standards. Then, in Subsection 4.2, we use a systematic literature review (SLR) to discover current privacy-by-design techniques. The resulting mappings are a comprehensive analysis of privacy legislation and technical requirements so that PriVARq operation guarantees better PII protection than any similar architecture.

4.1. Actor-Requirement Mapping using Personal Data Protection Legislation and Security Standards

During the review of the GDPR and the Ecuadorian LOPDP along with the NIST SP 800-53 and ISO 27001 security standards, different actors and requirements were identified. Actors interact from the beginning of the PII collection process until their verification. A design constraint at this point is to unify roles to guarantee an adequate segregation level and reduce authorization creep. Such role definition is highly dependent on the level of granularity during the analysis of privacy-preserving laws and security standards. Subsection 5.1 presents a detailed explanation of the identified Actors. Meanwhile, Requirements were identified by using a systematic literature review (SLR) to analyze the previous documents, applying the Kitchenham approach (Kitchenham et al., 2009). Such requirements

encompass how privacy-preserving services are deployed and the respective functional constraints associated with the architecture's operation. Finally, in Subsection 5.2, a detailed mapping between requirements, privacy preserving laws, and security standards is presented.

4.2. Identifying Privacy-by-Design Techniques

We carried out an SLR to identify privacy-by-design techniques, following the methodology proposed by Kitchenham (Kitchenham et al., 2009).

4.2.1. Research Questions

We proposed the following research questions to identify current privacy-by-design techniques or solutions that could help implement PriVARq:

RQ1: What privacy-by-design techniques or solutions have been proposed in the last five years?

RQ2: What privacy-by-design techniques or solutions are the most used?

RQ3: Which of the identified privacy-by-design techniques or solutions are oriented to implement a privacy-oriented architecture?

4.2.2. Search Process

A simple search was done through Google Scholar, considering digital libraries such as IEEE Xplore, ACM, Springer-link, among others. Software engineering and computer science were disciplines considered in the search, but using "privacy-by-design" keywords to restrict the results.

4.2.3. Selection Process

The following is a set of inclusion and exclusion criteria for the selection of articles. Only full-research papers were considered:

- The tile must include the keywords.
- Articles must be written in English or Spanish.
- Ad-hoc solutions were disregarded as we are focused on general architecture proposals.
- Articles must be strictly related to privacy-by-design within the aforementioned disciplines.
- Articles must be written in the last 5 years, i.e., between 2018 and 2022.
- Articles must have verified citations.

In Figure 1, the search and selection process is summarized.

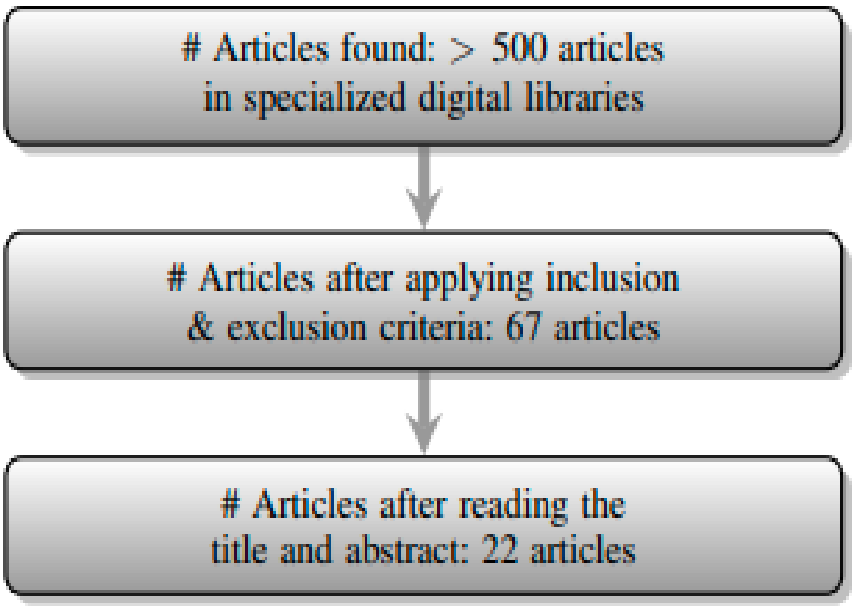

Figure 1: Article search & Selection process

At the beginning, we found more than 500 articles. Then, after applying the exclusion and inclusion criteria, we obtained 67 articles. Finally, after reading the title and abstract, only 22 articles were identified that matched the relevant criteria, excluding posters, short papers, and ad-hoc solutions. Appendix 1 contains the bibliographic information of the selected articles.

4.2.4. Result Analysis

The process' outcome captured the privacy-by-design techniques used in each article. Subsequently, we answered the proposed research questions based on the 22 selected articles.

RQ1: *What privacy-by-design techniques or solutions have been proposed in the last five years?*

In the last five years, several methodologies, architectures and techniques have been proposed to implement privacy-by-design. These techniques provide organizations and developers with a foundation to build privacy-focused systems and applications that comply with privacy regulations such as the GDPR and the LOPDP. Furthermore, by incorporating them into their processes, businesses can create more trustworthy and privacy-respecting products and services. Table 1 summarizes our findings based on the analysis of the selected articles. Curiously, techniques T4. Blockchain and T7. Smart Contracts, which are not privacy-preserving per se, have been used for automating and enforcing the terms of contracts in a transparent and immutable manner. As a consequence, one may argue that these techniques pose privacy challenges as they are more focused on data security and integrity. Thus, for privacy-by-design purposes, we advise to take careful considerations when designing systems based on these techniques since additional privacy-enhancing technologies or techniques should be employed to ensure that personal data is adequately protected while remaining compliant with relevant data protection laws and regulations.

Table 1: Privacy-by-design techniques

ID	Technique	Description
T1	Trust Agents	A trust agent encapsulates the owner's authentication data, possibly using multiple factors, and controls the owner's digital identities contained therein.
T2	Anonymization	It aims to prevent direct identification of individuals by removing all PII
T3	Transparent Data Policies	Privacy Policies that are well-defined, clear and easily understandable to inform individuals about how their data will be used, shared, and protected, fostering transparency and trust.
T4	Blockchain	It is a distributed data structure that records transactions across multiple computers in a secure and immutable manner. It operates as a chain of blocks, where each block contains a list of transactions.
T5	Awareness	It is the education, communication, and training on PII privacy issues for individuals to understand the risks associated with mishandling their PII.
T6	Consent Management	These systems ensure that individuals can easily provide, withdraw, or modify their consent to the collection and processing of their personal data.
T7	Smart Contracts	It is a self-executing computer program that is used to automate the execution of an agreement so that all participants can be immediately sure of the outcome without the involvement of a third party or loss of time. It can also automate a workflow, triggering the following action when conditions are met.
T8	Attribute-level Privacy Control	It is a kind of access control based on the attributes of the person. If the individual meets the attributes specified for access, the access will be provided; otherwise, it will be denied.
T9	Encryption	Method for securely sharing data over an insecure communication media, making the message unreadable to any unauthorized person.
T10	Onion Routing	Anonymous communication over an onion network where each message per layer is encapsulated with encryption. Each onion router decrypts one layer at a time before reading the message.
T11	Location Granularity	Users can choose the collection accuracy of their location data
T12	Forensic Information	Collect information on resources used by computer systems, identity managers, threat defense, and security components.
T13	Data Minimization	It focuses on reducing personal details as much as possible when processing PII without undermining its utility.
T14	Concealment	A mechanism to preventing PII from being made public or known.
T15	Legal Ontologies	It is a data model of legal knowledge of privacy agents, data types, types of processing operations, rights and obligations, and the relationships between those concepts.
T16	Data Breach Notification Pattern	It is a prompt and detailed user notification about a data leak.
T17	Compliance Policy	This policy is related to the documentation of processes, audits, and compliance with PII protection laws.
T18	Differential Privacy	It is a mechanism to share information from a dataset so that insignificant changes are made to the original data to prevent inference of any information about its owner.
T19	Inferential Privacy	It guarantees that anyone who accesses a dataset must reach the same conclusion as any other person who does not have access to the same dataset.
T20	Identity Protection	It is the protection provided to PII or identity to prevent fraud. It can be achieved by applying passwords, digital certificates, or biometrics.
T21	Privacy-Preserving Proxy	Interpreting privacy policies written in standard language to preserve privacy between members of a computer network.
T22	Petri Nets	A modeling approach for the visual representation of processes in terms of states and transitions helps the developer to understand the system.
T23	Hardware-based Security	Physical security uses hardware instead of software. For example, the protection of machines, peripherals, and physical devices through security cameras, and locks.
T24	Separation	It refers to the distribution of PII as much as possible to avoid correlation.
T25	Distributed Hash Table	Decentralized and scalable data store containing tuples ⟨key, value⟩. It supports put and get functions just like hash tables.
T26	Single Point of Contact	Department or person that handles all requests and inquiries.
T27	XACML	Extensible Access Control Language that defines an attribute-based access control policy language, an architecture, and a processing model to evaluate access requests.
T28	XSLT	It is a language that allows transforming XML documents into other XML documents with different formats, such as plain text.

RQ2: *What privacy-by-design techniques or solutions are the most used?*

During the SLR, we found that the most used privacy-by-design technique is Data Minimization, which is covered in 12 articles, followed by the Encryption technique, which is covered in 9 articles. Figure 2 shows the top ten privacy-by-design techniques (identified in Table 1) classified by the number of occurrences in the literature.

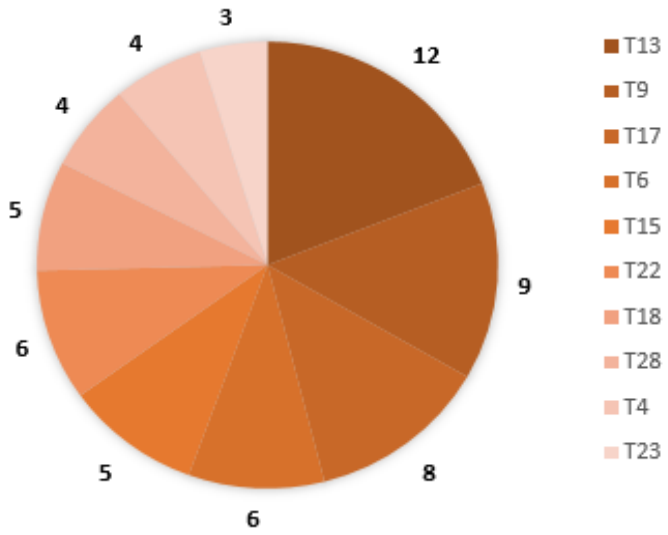

Figure 2: Privacy-by-design techniques by number of occurrences

RQ3: *Which of the identified privacy-by-design techniques or solutions are oriented to implement a privacy-oriented architecture?*

Implementing a privacy-oriented architecture requires integrating various privacy-by-design techniques and solutions to ensure that privacy is built into the system's design. By combining the privacy-by-design techniques and solutions identified in Table 1, organizations can create a privacy-oriented architecture that respects individuals' privacy rights and complies with relevant data protection laws and regulations. In Section 5, we identify the privacy requirements that a privacy-oriented architecture should consider in order to map them with the *Ti* techniques identified in Table 1.

5 Introducing PriVARq

This section introduces our privacy-oriented architecture PriVARq for the collection, processing, verification, and transference of PII. We start by defining the actors and requirements that PriVARq should fulfill based on legal instruments (LOPDP and GDPR) and information security standards (NIST SP 800-53 and ISO 27001). We then analyze privacy-by-design techniques, i.e., implementation solutions, in order to meet these requirements. Finally, we describe PriVARq and its components.

5.1. Actors

Table 2 shows the mappings between the privacy protection laws and the security standards. By analyzing these relationships, we can specify the functions of seven well-defined actors (*An*) that actively participate in the collection, processing, verification, and transference of PII.

Table 2: Identification of actors in the privacy protection laws and security standards

Actors	GDRP	LOPDP	NIST SP 800-53	ISO 27001
A1. Data Owner	Articles: 1, 4, 9, 12, 24, 25, 27, 44, 49, 51, 54, 57, 62,78, 82, 91, 95, 98. Recitals: 1-3, 5, 7, 8, 10, 12-15, 18, 21, 23, 24, 26, 30, 34, 35, 39, 46, 53, 54, 57, 71, 75, 77, 80, 84-86, 91, 94, 98, 111, 113, 115-117, 123, 132, 143, 146, 148, 154, 166, 170.	Articles: 2-5, 7-10, 12-17, 19-21, 24, 26-31, 33, 36, 39, 41, 42, 46, 47, 50, 57, 58, 60, 62-64, 67-69, 75-77. General Dispositions: Seventh; Second Reformatory	N/A	Controls: A.9.3, A.12.1, A.13.2, A.13.2.4, A.16.1
A2. Data Controller	Articles: 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27,28 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 42, 43, 44, 46, 47, 48, 49, 51, 56, 57, 58, 60, 62, 65, 70, 79, 81, 82, 83, 85, 90. Recitals: 10, 13, 18, 22, 23, 24, 25, 26, 28, 29, 36, 39, 40, 41, 42, 43, 45, 47, 49, 50, 57, 59, 60, 61, 63, 64, 65, 66, 68, 69, 71, 73, 74, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 89, 90, 92, 94, 95, 97, 98, 99, 101, 108, 109, 113, 114, 115, 122, 124, 126, 127, 131, 132, 143, 144, 145, 146, 147, 148, 153, 156, 164, 168, 171, 173	Articles: 3, 4, 5, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 19, 20, 27, 30, 33, 34, 35, 36, 37, 39, 40, 41, 42, 43, 46, 47, 48, 49, 50, 51, 52, 53, 57, 58, 59, 62, 64, 66, 67, 68, 69, 70, 71, 72, 76. General Dispositions: Fourth	Sections: 1.2, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 3.4, 3.6, 3.7, 3.8, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17, 3.18, 3.20	Controls: A.6.1.1, A.6.1.5, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.3.1, A.8.1.3, A.9.1.2, A.9.2.6, A.11.2.9, A.12.1, A.13.2, A.13.2.4, A.15.1, A.16.1, A.17.1.2, A.18.1
A3. Data Processor	Articles: 3, 4, 13, 18, 23, 24, 27- 44, 46-49, 56-58, 60, 62, 65, 70, 79, 81-83, 85, 90. Recitals: 22-24, 28, 36, 77-83, 95, 97-99, 101, 108, 109, 114, 115, 122, 124, 126, 127, 131, 132, 143, 144- 148, 153, 164, 168.	Articles: 3-5, 7, 17, 19, 20, 30, 34, 35, 37, 40, 41, 43, 47-53, 57-59, 66, 67, 69-72, 76. General Dispositions: Sixth; Transitional First and Third	Sections: 1.2, 1.3, 2.1-2.5, 3.1-3.20	Controls: A.6.1.1, A.6.1.5, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.3.1, A.8.1.1, A.8.1.2, A.8.1.3, A.9.1.1, A.9.1.2, A.9.2.6, A.10.1.1, A.11.2.9, A.12.2, A.12.6, A.13.1, A.13.2, A.14.1, A.15.1, A.16.1, A.17.1.2, A.18.1, A.18.2
A4. Delegate	The delegate is considered a data controller in this regulation.	Articles: 4, 5, 12, 47, 48, 49, 50, 58 y 76.	Sections: 1,2, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 3.4, 3.6, 3.7, 3.8, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17, 3.18, 3.20	Controls: A.6.1.1, A.6.1.5, A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.3.1, A.8.1.1, A.8.1.2, A.8.1.3, A.9.1.1, A.9.1.2, A.9.2.6, A.11.2.9, A.12.6, A.13.1, A.13.2, A.15.1, A.16.1, A.17.1.2, A.18.1,.18.2
A5. Recipient	Articles: 4, 13, 14. Recitals: 47, 69	Articles: 4, 5, 12, 14, 33 y 51.	N/A	Controls: A.7.2.2, A.9.1.2, A.9.2.6, A.11.2.9, A.13.2, A.15.1, A.16.1, A.17.1.2, A.18.1
A6. Control Authority	Articles: 4, 6, 10, 12-15, 27, 28, 30, 31, 33-37, 39-43, 45-47, 49-68, 70, 74, 75, 77-80, 83, 85, 90, 91, 97 Recitals: 13, 20, 36, 79, 80-82, 84-86, 89, 91, 94-96, 108, 112, 113, 116-139, 141-144, 148, 150, 151, 153, 164, 168, 171	Articles: 4-6, 10, 17, 24, 28, 30-35, 37, 41-43, 47-59, 61, 63-72, 74-76. General Dispositions: First, Fourth and Fifth	N/A	Controls: A.6.1.3, A.16.1.1, A.18.1.5, A.9.2.6, A.11.2.9, A.13.2,A.15.1, A.16.1, A.18.1, A.18.2
A7. Certification Entity	Articles: 42, 43, 58, 64, Recitals: 100, 168	Articles: 54 y 66	N/A	Controls: A.11.2.9, A.15.1, A.18.1

A1. Data Owner: An identifiable natural person who owns their PII. The data owner and their PII are subject to treatment.

A2. Data Controller: Natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines or decides the different purposes and treatment of PII collected from the data owner.

A3. Data Processor: Natural or legal person, public or private authority, or other body that, alone or jointly with others, processes PII in the name and on behalf of a data controller.

A4. Delegate: Natural person in charge of informing the data controller or data processor about their legal obligations in data protection, ensuring or supervising the regulatory compliance. Also, this actor must cooperate with the Control Authority. The delegate is a point of contact between the Personal Data Protection Authority and the entity responsible for data processing.

A5. Recipient: Natural or legal person which PII has been transferred to.

A6. Control Authority: Independent public authority in charge of supervising the application of personal data protection legislation to protect the fundamental rights and freedom of data owners regarding the treatment of their personal data.

A7. Certification Entity: Entity recognized by the control authority, which may, on a non-exclusive basis, provide certifications regarding the protection of PII.

Each actor plays a specific role in the collection, processing, verification, and transference of PII. These roles are described in the privacy protection laws, GDPR and LOPDP, and security standards, NIST 800-53 and ISO 27001.

5.2. Requirements

In this section, we identify the privacy requirements that any privacy-preserving architecture such as PriVARq should fulfill for the collection, processing, verification, and transference of PII. Table 3 displays three of the identified privacy requirements with their corresponding mappings to the GDPR, LOPDP, NIST 800-53, and ISO 27001. A comprehensive list of all the identified privacy requirements (*Rj*), with their mappings, can be found in Appendix 2.

Table 3: Identification of requirements in the privacy protection laws and security standards

Requirement	GDPR	LOPDP	NIST SP 800-53	ISO 27001
R1. Processing and Data Treatment	Articles: 1-30, 32, 35-42, 44, 47, 51, 55, 56-58, 60, 62, 64, 71, 77, 79, 80, 81, 82, 85-89, 91, 94, 95, 98. Recitals: 1-4, 9-20, 22, 23, 26, 27, 29, 31-33, 36-40, 42-56, 58, 60-63, 65-84, 89-94, 96-98, 105, 104, 108, 113-115, 117, 122-124, 126-129, 131, 135, 139, 142, 144, 146, 153-156, 158-160, 162, 171, 173	Articles: 2- 4, 7-12, 14-19, 21, 24-26, 28, 30-39, 41, 42, 44, 45, 47-51, 53, 56-58, 65, 67-70, 76; Dispositions: General Ninth, Transitory Second	Sections: 3.6, 3.10, 3.15	Recitals: A.5.1.1, A.6.1.1, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2.1, A.8.2.3, A.8.3.1, A.8.3.2, A.9.4.1, A.14.3, A.17.2
R2. Confidentiality	Articles: 5, 28, 32, 38, 76. Recitals: 39, 49, 75, 83, 85, 162, 163	Articles: 10, 30, 31, 44, 45, 47, 70, Second Reformatory	Sections: 3.10, 3.11	Recitals: A.5.1.1, A.8.1.3, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.2, A.9.2.4, A.9.3.1
R3. Consent	Articles: 4, 6, 7, 8, 9, 13, 14, 17, 18, 20, 22, 40, 49, 83. Recitals: 32, 33, 38, 40, 42, 43, 50, 51, 54, 65, 68, 71, 111, 112, 155, 161, 171	Articles: 1, 7, 8, 10, 12, 15, 16, 17, 19, 20, 21, 26, 27, 30, 31, 33, 36, 60 Reformatory Fourth Replace	Sections: 2.1, 3.15	Recitals: A.8.1.3, A.8.2.1

These requirements can help design and implement technological solutions to preserve data privacy:

R1. Processing and Data Treatment: Collecting PII within a computing architecture must be done by the person in charge only after the data owner's consent is given. Any further processing and treatment of such information must be done confidentially, ensuring its availability, and integrity.

R2. Confidentiality: The PII stored must be kept private and without access to unauthorized personnel.

R3. Consent: This is a step prior to the delivery of PII by the data owner. The consent for collecting, treating, processing, and storing PII should include the data's use, duration, and purpose.

R4. Conservation and Disposal: PII must be stored only for the required time to fulfill the purpose for which it was collected. PII must be entirely deleted from all physical and logical storage forms once the treatment period has expired.

R5. Availability: PII must be available when accessed by authorized personnel, or when required by an authorized party, or when requested by the data owner.

R6. Minimization: Data controllers should limit the collection of PII to the minimum required only. This in order to fulfill a specific objective of the organization which must be disclosed before obtaining the data owner's consent.

R7. Integrity: The stored PII must not be modified or tampered with by unauthorized personnel.

R8. Portability and Transfer: PII should be portable prior consent, and upon request of the data owner. Such portability must be implemented using a compatible, updated, universal, machine-readable, and interoperable format for transference between data owners and data controllers.

R9. Transparency: PII should be easily accessible and understandable by using a plain and unambiguous language during its treatment.

R10. Risk Evaluation: Internal processes must be carried out to assess the risks and threats that could affect the normal operation of any architecture (such as PriVARq) during the collection, processing, verification and transference of PII.

R11. Consistency: Stored PII should be kept consistent as it is moved or processed over a computer network and between various participating applications within any architecture such as PriVARq.

5.3. Requirements and Privacy-by-Design Techniques

In Table 4, privacy-by-design techniques (*Ti*) and privacy requirements (*Rj*) are mapped. This mapping can help us fulfilling such requirements while keeping them consistent with the techniques identified through the SLR analysis explained in Section 3.3. As one can observe, *T15. Legal Ontologies* and *T17. Compliance Policies* are techniques which, if implemented, can meet most of the identified privacy requirements.

Table 4: Mapping of privacy-by-design techniques and privacy requirements

Req. / Tech.	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
T1		X					X				
T2	X					X					
T3			X						X	X	
T4					X		X				
T5	X		X								
T6	X	X	X	X				X		X	
T7							X				X
T8		X									
T9		X					X				
T10		X					X				
T11			X			X					
T12									X	X	
T13	X					X					
T14	X	X				X					
T15	X	X					X	X	X	X	X
T16			X								
T17	X	X	X	X	X		X	X		X	
T18	X										
T19	X		X								
T20		X	X								
T21		X									
T22	X	X		X			X		X	X	
T23		X			X		X				
T24	X					X					
T25					X		X				X
T26			X		X						
T27		X							X		X
T28	X	X						X	X		X

5.4. Components of PriVARq

For any organization, a security breach may threaten personal information in at least one of the following aspects (AEPD, 2022):

1. Uncontrolled third-party access.
2. Unauthorized insider access.
3. Increased privilege escalation and data manipulation due to authorization creep
4. Negligent or accidental destruction, manipulation and loss of data derived from privileged credential misuse.

Then, if any security incident arises during the collection, processing, verification, and transference of PII, privacy issues might also affect its owner's rights. To solve these flaws, Figure 3 depicts PriVARq, as a 4-component privacy-preserving architecture to aid the secure collection, processing, verification, and transference of PII.

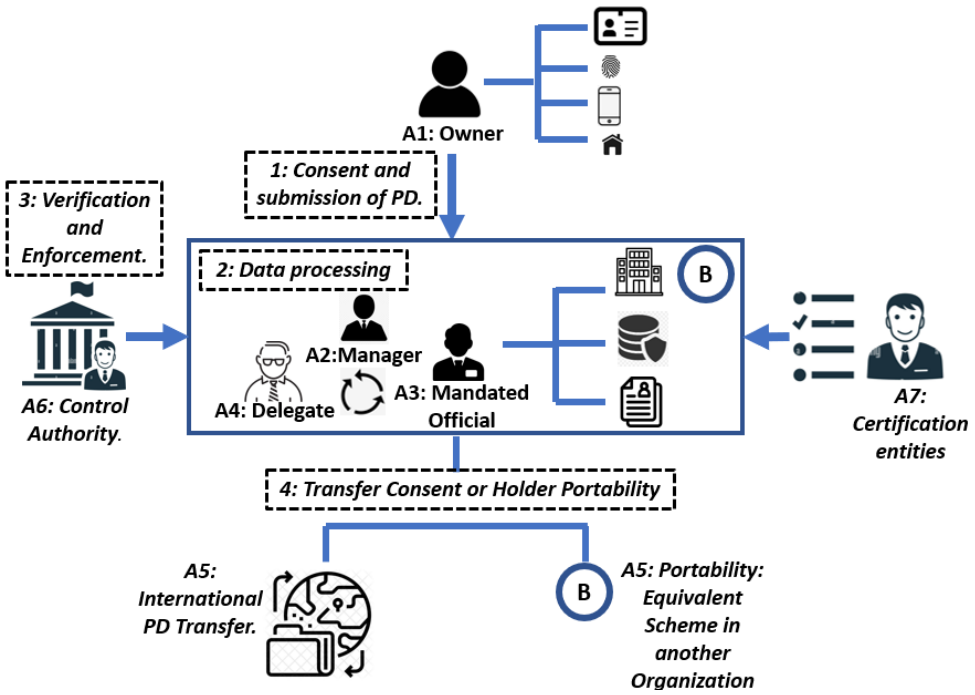

Figure 3: PriVARq: A 4-component privacy-preserving architecture for the secure collection, processing, verification and transference of PII

Component 1 - PII Collection: The data owner delivers his personal data freely and voluntarily to the data controller. The data controller has to explain to the data owner the rights, principles, and purpose for which their data is being collected.

Component 2 - PII Processing: After the collection process, the data controller sends the personal data collected from the owner to the data processor in printed or digital form. The data processor verifies that the data is complete, secure, and stored correctly. When PII has to be treated, data controllers are the ones who manipulate the stored data for the specific purpose of its collection. The delegate, entrusted by the organization, is permanently responsible for verifying compliance with the internal laws of the organization concerning personal information. The data controller, data processors, and delegate should work together to ensure such compliance.

Component 3 - PII Verification: The Control Authority is the governing body that will enforce all current Laws regarding the privacy protection of PII to comply with national and international regulations. The Control Authority will be able to financially fine organizations or companies that process PII when they do not comply with such regulations. The certification entity will entrust the data controller the implementation of such practices in its processes, aiming to promote the trust of the data owner through the Control Authority's technical regulations.

Component 4 - PII Transference: The transfer of PII between participating organizations (at national or international outreach) must be carried out with the prior consent of the data owner.

Finally, Table 5 maps privacy requirements to each component of PriVARq. Notice that PII processing (Component 2) and PII transference (Component 4) are vital components to protect data privacy because both components encompass the majority of the 11 privacy requirements.

Table 5: PriVARq Components and privacy requirements

Req. / Comp.	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
Component 1	X	X	X			X			X		X
Component 2	X	X		X	X	X	X	X	X	X	X
Component 3		X		X	X	X		X			
Component 4	X	X	X	X	X	X	X	X	X	X	X

6 Conclusion and Future Work

In this article, we have introduced PriVARq, a novel privacy-preserving architecture to aid PII's secure collection, processing, verification, and transference. To deploy PriVARq, we defined the actors, requirements, and privacy-by-design techniques based on personal data protection legislation proposed in Europe and Latin America, i.e., GDPR and LOPDP. Although it may be arguable that our proposed solution relies heavily in legal compliance for the resolution of privacy concerns in the treatment of PII, unlike similar approaches already discussed in Mistake! The source of the reference cannot be found., PriVARq ultimate goal is achieving balance between legal frameworks and technical requirements.

As a consequence, PriVARq, at its core, mitigates the flaws in existing legislation by introducing security techniques outlined in industry-leading standards such as the ISO 27001 and NIST 800-53. In addition, we carried out a systematic literature review to identify the privacy-by-design techniques that can be used to implement the 4 components of PriVARq. Our research shows that non-technical operational constraints such as Compliance Policies and Digital Consent are highly relevant for implementing PriVARq since they cover most of the identified privacy requirements. In general, PriVARq considers the actors and privacy requirements that must be fulfilled to protect PII and describes possible implementation techniques that can help organizations streamline the implementation process of data protection legislation.

Nonetheless, reports have demonstrated that, in most cases, information is being collected without consent, e.g., website trackers that follow Internet users from site to site to collect browsing information (Shapiro, 2022). In addition, studies have shown that data owners become fatigued with consent mechanisms (Utz, Degeling, Fahl, Schaub, & Holz, 2019); i.e., when consumers engage daily with numerous websites, making it impractical to read and agree to lengthy data usage agreements per each site. Despite the development of web-based tools to provide workarounds, such as the "I don't care about cookies" browser extension (Shapiro, 2022), a shortage of effective privacy consent solutions still remain unsolved. In fact, although the design components explained in Figure 3 may seem legally admissible, obtaining valid consent from data owners remains a challenge for deploying PriVARq in real-world situations. For future work, we will deploy PriVARq using the privacy-by-design techniques detailed in this article, not only providing specific technical details of its implementation, but also focusing on implementing better consent mechanisms during PII collection in order to facilitate privacy compliance and increase users' involvement in the whole PII treatment life cycle.

References

[1] Adnan, M., Kalra, S., Cresswell, J.C., Taylor, G.W., & Tizhoosh, H.R. (2022). Federated learning and differential privacy for medical image analysis. *Scientific Reports, 12*(1), 1953.

[2] AEPD (2022). Personal data gaps in the health sector. Spanish Data Protection Agency. https://www.aepd.es/en/prensa-y-comunicacion/blog/data-breaches-development-and-pre-production-enviroments.

[3] Agrawal, P., Singh, A., Raghavan, M., Sharma, S., & Banerjee, S. (2020). An operational architecture for privacy-by-design in public service applications. *CoRR*, 1-27.

[4] Alessi, M., Camillo, A., Giangreco, E., Matera, M., Pino, S., & Storelli, D. (2018). Make Users Own Their Data: A Decentralized Personal Data Store Prototype Based on Ethereum and IPFS. *Proceedings of the 3rd International Conference on Smart and Sustainable Technologies (SpliTech)*, 1–7.

[5] Alimonti, V., & Rodríguez, K. (2020). A Look-Back and Ahead on Data Protection in Latin America and Spain. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain

[6] Alkhariji, L., Alhirabi, N., Alraja, M.N., Barhamgi, M., Rana, O., & Perera, C. (2021). Synthesising Privacy by Design Knowledge Toward Explainable Internet of Things Application Designing in Healthcare. *ACM Transactions on Multimedia Computing, Communications, and Applications, 17*(2s), 1–29.

[7] Alshammari, M., & Simpson, A. (2018). A model- based approach to support privacy compliance. *Information and Computer Security, 26*(4), 437–453.

[8] Amankona, V., Asante, A., Opoku, M., Ohemeng-Gyaase, P., Srekumah, C., Peprah, A.K., & Amankwa- Danquah, P. (2021). Integrating Privacy-By-Design in e-Health. *Proceedings of the International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1–7.

[9] Anastasakis, Z., Psychogyios, K., Velivassaki, T., Bourou, S., Voulkidis, A., Skias, D., Gonos, A., and Zahariadis, T. (2022). Enhancing Cyber Security in IoT Systems using FL-based IDS with Differential Privacy. *Proceedings of the Global Information Infrastructure and Networking Symposium (GIIS)*, 30–34.

[10] Andrade, V.C., Gomes, R.D., Reinehr, S., Freitas, C.O.D.A., & Malucelli, A. (2023). Privacy by Design and Software Engineering: a Systematic Literature Review. *Proceedings of the XXI Brazilian Symposium on Software Quality*, 1-10.

[11] Angarita, N.R. (2012). Constitutional approach to the protection of personal data in Latin America. *Revista Internacional de Protección de datos personales*, 1-13.

[12] Arfaoui, S., Belmekki, A., & Mezrioui, A. (2021). A Privacy by Design Methodology Application in Telecom Domain. *International Journal of Communication Networks and Information Security, 13*(2), 184–198.

[13] Arfaoui, S., Mezrioui, A., & Belmekki, A. (2020). A Methodology for Assuring Privacy by Design in Information Systems. *International Journal of Communication Networks and Information Security, 12*(3), 364–375.

[14] Ariganello, J. (2022). Why are Organizations Suffering from a Lack of Threat Intelligence Information? *Anomali Blog*. https://www.anomali.com/blog/why-are-organizations-suffering-from-lack-of-threat-intelligence-information

[15] Cao, H., Liu, S., Wu, L., Guan, Z., & Du, X. (2019). Achieving differential privacy against non-intrusive load monitoring in smart grid: A fog computing approach. *Concurrency and Computation: Practice and Experience, 31*(22).

[16] Cohen, J.E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Georgetown Law Faculty Publications and Other Works, 810*, 1373–1438.

[17] Distri Net, R.G. (2020). LINDDUN privacy engineering: Systematic elicitation and mitigation of privacy threats in software systems. LINDDUN. https://linddun.org/

[18] Diver, L., & Schafer, B. (2017). Opening the black box: Petri nets and Privacy by Design. *International Review of Law, Computers & Technology, 31*(1), 68-90.

[19] Dong, J., Roth, A., & Su, W.J. (2022). Gaussian Differential Privacy. *Journal of the Royal Statistical Society Series B: Statistical Methodology, 84*(1), 3–37.
[20] Dorri, A., Kanhere, S.S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 618–623.
[21] EC-Council (2022). Why Organizations Need to Deliberately Adopt Threat Intelligence. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/organization-threat-intelligence-siem-soar/
[22] ESGInnova (2022a). ISO 27001: ISO 27001 Management Systems software. ISO Tools.
[23] ESGInnova (2022b). ISO 27002: The importance of Good Practices in Information Security Systems.
[24] European Union (2003). Commission Decision of June 30, 2003 on the adequacy of the protection of personal data in Argentina. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32003D0490
[25] European Union (2019). Official legal text GDPR. https://gdpr-info.eu/
[26] Fortinet (2022). Risk increases with cybersecurity skills gap, while 87% of Latin American companies report having been hacked in the last year. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortinet-annual-skills-gap-report-uncovers-increase-breaches-attributed-to-lack-of-cybersecurity-skills
[27] Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research, 59*(6), 703–705.
[28] Hernandez, J., McKenna, L., & Brennan, R. (2021). TIKD: A Trusted Integrated Knowledge Dataspace for Sensitive Healthcare Data Sharing. *Proceedings of the 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, 1855–1860.
[29] Herrera Carpintero, P. (2016). The right to private life and social networks in Chile. *Revista chilena de derecho y tecnología, 5*(1), 87–112.
[30] ISO/IEC (2020). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems - Requirements. https://www.iso.org/standard/27001
[31] Kapoor, A. (2020). Operationalizing privacy by design: An Indian illustration. https://dx.doi.org/10.2139/ssrn.3805402
[32] Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology, 51*(1), 7–15.
[33] Kumar, R., & Tripathi, R. (2021). Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. *The Journal of Supercomputing, 77*(8), 7916–7955.
[34] Luxon, B. (2021). Why organizations need threat intelligence tools as part of their security defences. GetSignal.info. https://www.getsignal.info/blog/threat-intelligence-in-corporate-security
[35] Megías, D., Kuribayashi, M., Rosales, A., Cabaj, K., & Mazurczyk, W. (2022). Architecture of a fake news detection system combining digital watermarking, signal processing, and machine learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *13*(1), 33-55.
[36] Mikkonen, T. (2014). Perceptions of controllers on EU data protection reform: A Finnish perspective. *Computer law & security review*, *30*(2), 190-195.
[37] Ministry of Citizenship Brazil (2018). General personal data protection law (LGPD). https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd.

[38] Morris, A., & Lessio, N. (2018). Deriving privacy and security considerations for core: An indoor iot adaptive context environment. *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, 2–11.

[39] Nicholson, J., & Tasker, I. (2017). Data exchange: Privacy by design for data sharing in education. *Proceedings of the International Conference on the Frontiers and Advances in Data Science (FADS)*, 92–97.

[40] O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia computer science, 113*, 653–658.

[41] Pedroza, G., Muntes-Mulero, V., Martín, Y.S., & Mockly, G. (2021). A model-based approach to realize privacy and data protection by design. *Proceedings of the European Symposium on Security and Privacy Workshops (EuroS&PW)*, 332–339.

[42] Pillitteri, V. (2022). Assessing security and privacy controls in information systems and organizations. NIST. https://csrc.nist.gov/pubs/sp/800/53/a/r5/final

[43] Piras, L., Al-Obeidallah, M.G., Pavlidis, M., Mouratidis, H., Tsohou, A., Magkos, E., & Praitano, A. (2021). A data scope management service to support privacy by design and gdpr compliance. *Journal of Data Intelligence*, *2*(2), 136–165.

[44] Piras, L., Al-Obeidallah, M.G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J.B., Fiorani, M., Magkos, E., Sanz, A.C., Pavlidis, M., D'Addario, R., & Zorzino, G.G. (2019). DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance. *Trust, Privacy and Security in Digital Business*, 78–93.

[45] Registro Oficial Ecuador (2021). Organic law on personal data protection. https://www.registroficial.gob.ec/index.php/

[46] Robles, T., Bordel, B., Alcarria, R., and Sánchez- de Rivera, D. (2020). Enabling trustworthy personal data protection in ehealth and well- being services through privacy-by-design. *International Journal of Distributed Sensor Networks*, *16*(5), 1-23.

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

[48] Shapiro, J. (2022). Why Digital Privacy Is So Complicated. Progressive Policy. https://www.progressivepolicy.org/wp-content/uploads/2022/05/PPI_Why-is-Digital-Privacy-So-Complicated_FINAL.pdf

[49] Sirus, S., Nurse, J., & Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, 88-95.

[50] Teresa Baldassarre, M., Santa Barletta, V., Caivano, D., & Piccinno, A. (2021). Integrating security and privacy in HCD-scrum. *Proceedings of the 14th Biannual Conference of the Italian SIGCHI Chapter*, 1-5.

[51] Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys, 51*(2), 1-27.

[52] Toth, K.C., & Anderson-Priddy, A. (2019). Privacy by design using agents and sovereign identities. *Proceedings of the Information Security and Privacy Protection Conference*, 73-94.

[53] UASB (2022). Data Protection. Universidad Andina Simón Bolívar. https://www.uasb.edu.ec/ciberderechos/proteccion-de-datos/

[54] Ujcich, B.E., & Sanders, W.H. (2019). Data protection intents for software-defined networking. *Proceedings of the Conference on Network Softwarization (NetSoft)*, 271–275.

[55] Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un) informed consent: Studying GDPR consent notices in the field. *Proceedings of the ACM SIGSAC conference on computer and communications security*, 973-990.

[56] Volodina, E., Mohammed, Y.A., Derbring, S., Matsson, A., & Megyesi, B. (2020). Towards privacy by design in learner corpora research: A case of on-the- fly pseudonymization of

swedish learner essays. *Proceedings of the 28th International Conference on Computational Linguistics*, 357–369.

[57] Wahlstrom, K., Ul-haq, A., & Burmeister, O. (2020). Privacy by design. *Australasian Journal of Information Systems, 24*. https://doi.org/10.3127/ajis.v24i0.2801

[58] Wang, S., Zhang, D., & Zhang, Y. (2019). Blockchain- based personal health records sharing scheme with data integrity verifiable. *IEEE Access, 7*, 102887-102901.

[59] Wirth, C., & Kolain, M. (2018). Privacy by blockchain design: a blockchain-enabled GDPR - compliant approach for handling personal data. *Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies*. https://doi.org/10.18420/blockchain2018_03

[60] Wuyts, K., Sion, L., & Joosen, W. (2020). Linddun Go: A lightweight approach to privacy threat modeling. *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, 302–309.

[61] Zarrabi F., & Brimicombe, A. (2019). A semantic rule-based approach for software privacy by design. *International Journal of Advances in Electronics and Computer Science, 6*(5), 30–37.

Authors Biography

Adán F. Guzmán-Castillo

Adán F. Guzmán-Castillo is a Computer Systems Engineer, Escuela Politecnica Nacional, Ecuador. Graduated with a Master's Degree in Computer Science, Escuela Politecnica Nacional, Ecuador. He is a researcher with experience in Artificial Intelligence, Data Science, Internet of Things and Information Technology. Adan is an Associate Engineer in the Information Technology Department of an Oil Company. His research interests are focused on the field of Data Science, Machine Learning and Technologies applied to medical sciences.

Gabriela Suntaxi

Gabriela Suntaxi is a researcher and professor in the Department of Informatics and Computer Science at the National Polytechnic School of Ecuador. Her research interests include privacy-preserving, query processing, information security, secure storage of outsourced databases and database auditing. She did her PhD studies at the Karlsruhe Institute of Technology, Germany. She holds a Master degree in Information Security from Macquarie University, Australia.

Bryan N. Flores-Sarango

Bryan N. Flores-Sarango is a Software Engineer and SOC Analyst at an TI services company. His research interests include data privacy, threat intelligence, and analytics optimization of security events. He completed his software engineering studies at the Escuela Politécnica Nacional and is a certified splunk engineer.

Denys A. Flores

Denys A. Flores is a Doctor of Philosophy in Computer Science, University of Warwick, UK. Masters degree with Distinction in Forensic Computing and Security, University of Derby, UK. He is an experienced consultant in Digital Forensics, IS Auditing and Information Security. Denys is an associate professor in the Department of Informatics and Computer Science at the National Polytechnic School of Ecuador. His research interests are in the field of Proactive Digital Forensics, and its application on a variety of fields, including money laundering detection, fraud detection, database auditing and evidence admissibility.

Appendix A: Articles Covered in the SLR between 2018 and 2022

Index	Authors	Title	Year	Publisher
A1	Wahlstrom, K.; Ul-haq, A.; Burmeister, O.	Privacy by design (Wahlstrom et al., 2020)	2020	Australian Computer Society
A2	Alkhariji, L.; Alhirabi, N.; Alraja, M.; Barhamgi, M.; Rana, O.; Perera, Ch.	Synthesising privacy by design knowledge toward explainable internet of things application designing in healthcare (Alkhariji et al., 2021)	2021	ACM
A3	Robles, T.; Bordel, B.; Alcarria, R.; S´anchez-de-Rivera, D.	Enabling trustworthy personal data protection in eHealth and well-being services through privacy-by-design (Robles et al., 2020)	2020	SAGE Publications
A4	Diver, L.; Schafer, B.	Opening the black box: Petri nets and Privacy by Design (Diver and Schafer, 2017)	2017	Taylor y Francis
A5	Nicholson, J.; Tasker, I.	Dataexchange: Privacy by design for data sharing in education (Nicholson and Tasker, 2017)	2017	IEEE
A6	Wirth, Ch.; Kolain, M.	Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data (Wirth and Kolain, 2018)	2018	European Society for Socially Embedded Technologies (EUSSET)
A7	Arfaoui, S.; Mezrioui, A.; Belmekki, A.	A Methodology for Assuring Privacy by Design in Information Systems (Arfaoui et al., 2020)	2020	Kohat University of Science and Technology (KUST)
A8	Amankona, V.; Asante, A.; Opoku, M.; Ohemeng-Gyaase, P.; Srekumah, C.; Peprah, A.; Amankwa-Danquah, P.	Integrating Privacy-By-Design in e-Health (Amankona et al., 2021)	2021	IEEE
A9	Arfaoui, S.; Belmekki, A.; Mezrioui, A.	A Privacy by Design Methodology Application in Telecom Domain (Arfaoui et al., 2021)	2021	Kohat University of Science and Technology (KUST)
A10	Agrawal, Prashant; Singh, Anubhutie; Raghavan, Malavika; Sharma, Subodh; Banerjee, Subhashis	An operational architecture for privacy-by-design in public service applications (Agrawal et al., 2020)	2020	arXiv
A11	Benhamida, F.; Navarro, J.; G´omez-Carmona, O.; Casado-Mansilla, D.; L´opez-de-Ipi˜na, D.; Zaballos, A.	PyFF: A Fog-Based Flexible Architecture for Enabling Privacy- by-Design IoT-Based Communal Smart Environments (Benhamida et al., 2021)	2021	Multidisciplinary Digital Publishing Institute
A12	Piras, L.; Al-Obeidallah, M.; Pavlidis, M.; Mouratidis, H.; Tsohou, A.; Magkos, E.; Praitano, A.	A Data Scope Management Service to Support Privacy by Design and GDPR Compliance (Piras et al., 2021)	2021	Rinton Press
A13	Kapoor, A.	Operationalizing Privacy by Design: An Indian illustration (Kappor, 2021)	2021	SCRIPTed
A14	Zarrabi, F.; Brimicombe, A.;	A Semantic Rule-Based Approach for Software Privacy by Design (Zarrabi and Brimicombe, 2019)	2019	Institute of Research and Journals
A15	Pedroza, G.; Muntes-Mulero, V.; Martin, Y.; Mockly, G.	A Model-based approach to realize privacy and data protection by design (Pedroza et al., 2021)	2021	IEEE
A16	Kumar, R.; Tripathi, R.	Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology (Kumar and Tripathi, 2021)	2021	Springer
A17	O'Connor, Y.; Rowan, W.; Lynch, L.; Heavin, C.	Privacy by design: informed consent and internet of things for smart health (O'Connor et al., 2017)	2017	Elsevier
A18	Volodina, E.; Mohammed, Y.; Derbring, S.; Matsson, A.; Megyesi, B.	Towards privacy by design in learner corpora research: A case of on-the-fly pseudonymization of swedish learner essays (Volodina et al., 2020)	2020	Proceedings of the 28th International Conference on Computational Linguistics
A19	Toth, K.; Anderson-Priddy, A.	Privacy by design using agents and sovereign identities (Toth and Anderson-Priddy, 2019)	2019	Information Security and Privacy Protection Conference (IFIP-SEC)
A20	Anastasakis, Z.; Psychogyios, K.; Velivassaki, T.; Bourou, S.; Voulkidis, A.; Skias, D.; Zahariadis, T.	Enhancing Cyber Security in IoT Systems using FL-based IDS with Differential Privacy (Anastasakis et al., 2022)	2022	IEEE
A21	Adnan, M.; Kalra, S.; Cresswell, J. C.; Taylor, G. W.; Tizhoosh, H. R.	Federated learning and differential privacy for medical image analysis (Adnan et al., 2022)	2022	Nature Publishing Group UK London
A22	Dong, J.; Roth, A.; Su, W. J.	Gaussian differential privacy (Dong et al., 2022)	2022	Oxford University Press

Appendix B: Identification of Requirements in the Privacy Protection Laws and Security Standards

Requirement	GDPR	LOPDP	NIST 800-53	ISO 27001
R1. Processing and Data Treatment	Articles: 1-30, 32, 35-42, 44, 47, 51, 55, 56-58, 60, 62, 64, 71, 77, 79, 80, 81, 82, 85-89, 91, 94, 95, 98. Recitals: 1-4, 9-20, 22, 23, 26, 27, 29, 31-33, 36-40, 42-56, 58, 60- 63, 65-84, 89-94, 96-98, 105, 104, 108, 113-115, 117, 122-124, 126-129, 131, 135, 139, 142, 144, 146, 153-156, 158-160, 162, 171, 173	Articles: 2- 4, 7-12, 14-19, 21, 24-26, 28, 30-39, 41, 42, 44, 45, 47-51, 53, 56-58, 65, 67-70, 76; Dispositions: General Ninth, Transitory Second	Sections: 3.6, 3.10, 3.15	Recitals: A.5.1.1, A.6.1.1, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2.1, A.8.2.3, A.8.3.1, A.8.3.2, A.9.4.1, A.14.3, A.17.2
R2. Confidentiality	Articles: 5, 28, 32, 38, 76. Recitals: 39, 49, 75, 83, 85, 162, 163	Articles: 10, 30, 31, 44, 45, 47, 70, Second Reformatory	Sections: 3.10, 3.11	Recitals: A.5.1.1, A.8.1.3, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.2, A.9.2.4, A.9.3.1
R3. Consent	Articles: 4, 6, 7, 8, 9, 13, 14, 17, 18, 20, 22, 40, 49, 83. Recitals: 32, 33, 38, 40, 42, 43, 50, 51, 54, 65, 68, 71, 111, 112, 155, 161, 171	Articles: 1, 7, 8, 10, 12, 15, 16, 17, 19, 20, 21, 26, 27, 30, 31, 33, 36, 60, Reformatory Fourth Replace	Sections: 2.1, 3.15	Recitals: A.8.1.3, A.8.2.1
R4. Conservation and Disposal	Articles: 12, 27, 54	Articles: 10, 12, 15, 17, 18, 27, 29, 34, 35, 51, 65	Sections: 3.19 Control Number: AC-3-4-16, AU-7-9, CP-9, IR-4, SA-8-20, SC-4, SI-13-14, MP-5, PM-21-22, SI-21-18-22	Recitals: A.8.1.2, A.8.3.1, A.8.3.1, A.8.3.2, A.12.4.4, A.17.1
R5. Availability	Articles: 32. Recitals: 49, 108	Articles: 1, 12, 13, 22, 23, 29, 37, 70	Sections: 1.5, 2,4, 3.13 Control Number: AC-2-7-17, AU-4-11, CA-5-7, CM-2-3-6-8, CP-7-8-9, IA-5, IR-7, PE-14-8-9, PM-11, RA-2-3, SA-8-10, SC-6-12-24-27-36-37-40, SI-2-3-8-14	Recitals: A.6.1.4, A.8.2.1, A.8.3.1, A.12.7.1, A.13.1.1, A.14.1.1, A.15.1.1, A.16.1.2, A.17.2
R6. Minimization	Articles: 5, 25, 47, 89 Recitals: 156	Articles: 7, 9, 10, 21, 26	Sections: 3.15	N/A
R7. Integrity	Articles: 5, 32. Recitals: 49, 112, 121	Articles: 10, 14, 18, 19, 27, 29, 37, 70	Sections: 3.19	Recitals: A.8.2.1, A.8.3.1, A.9.4.5, A.10.1, A.11.2.4, A.12.5, A.12.6.2, A.13.1.1, A.13.2.1, A.14.1.1, A.14.2.2-A.14.2.4, A.15.1.1, A.16.1.2, A.16.1.7, A.17.2.1
R8. Portability and Transfer	Articles: 4, 13-15, 20, 23, 28, 30, 40, 42, 44-49, 70, 83, 85, 88, 96, 97, Recitals: 6, 48, 68, 73, 101-103, 107, 110-115, 153, 156	Articles: 12, 17, 18, 55, 56, 5, 7, 59, 60	Sections: 2.2 Control Number: SC-27, AC-2-4-12, AU-4-10, CA-3, CM-7, CP-2-7-9, MA-6, MP-8, SC-4, SI-4-13	Recitals: A.5.1.1, A.6.1.4, A.8.1.4, A.8.2.1, A.8.2.3, A.8.3.1, A.8.3.3, A.13.2, A.17.1, A.17.2
R9. Transparency	Articles: 5, 88 Recitals: 13, 39, 58, 78, 100	Articles: 8, 9;10, 12, 34, 35	Sections: 3.15 Control Number: AT-3, CA-3, CP-8, PM-22-27, PT-1, SA-4, SR-5	N/A
R10. Risk Evaluation	Articles: 4, 23-25, 27, 30, 32-34, 36, 39, 49, 57, 70, Recitals: 9, 15, 28, 35, 38, 39, 51, 65, 71, 74-77, 80, 81, 83-86, 89, 91, 90, 96, 98, 116, 122, 144	Articles: 2, 9-11, 20, 37, 39, 40-44, 46, 47, 49, 60, 68, 76	Sections: 1.1, 1.2, 1.3, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17, 3.18, 3.19, 3.20	Recitals: A.6.1.1, A.6.1.2, A.6.1.5, A.6.2.1, A.7.1.1, A.8.1.1, A.8.2.1, A.8.3.1, A.8.3.2, A.9.1.1, A.9.1.2, A.9.2.6, A.9.4.2, A.10.1.1, A.11.1.1, A.11.2.1, A.11.2.6, A.11.2.7, A.11.2.9, A.12.1.4, A.12.2.1, A.12.6.1, A.12.5.1, A.12.6.2, A.13.1.3, A.14.1.1-A.14.1.3, A.14.2.2, A.14.2.4-A.14.2.6, A.15.1.1- A.15.1.3, A.15.2.2, A.17.2.1, A.18.2.3
R11. Consistency	Articles: 28, 35, 41, 46, 47, 51, 57, 60, 63, 66, 70, 74, 78, 85, 97 Recitals: 81, 119, 130, 135, 136, 138, 150, 153, 173	Articles: 10, 19, 29	Sections: 3.10	Recitals: A.8.2.3, A.8.3.1, A.17.2