*i** to Support Personal Data Protection Compliance

Jackeline Fernández[1], Carolina Sacoto[1], Karina Abad[1], Juan Pablo Carvallo[1]

[1] *CEDIA, Cuenca, Ecuador*

Abstract

As Information Systems become increasingly complex and ubiquitous, ensuring the security and privacy of personal data has become paramount. The need to protect individuals' privacy has led to the development of new laws and regulations, such as the General Data Protection Regulation in the European Union. This paper, presents an *i** based approach to support Personal Data Protection compliance. The proposal makes use of the DHARMA method aimed at the definition of Enterprise Systems Architecture. Additional activities have been added to the method to thoroughly review dependencies in order to identify and categorize potential risks associated to personal data treated by them and analyze appropriate actions to mitigate their impact. The resulting method, DHARMA-PDP, helps organizations ensure compliance with existing regulations and implement best practices to protect personal data.

Keywords 1

DHARMA Method, Personal Data Protection, Information Systems, Enterprise Systems Architecture, Compliance.

1. Introduction

Information Systems (IS) play a crucial role in our daily lives, facilitating automated interactions between organizations and individuals. The advent of modern technologies such as smart devices, cloud computing, artificial intelligence, and data analytics has made IS increasingly complex. However, this complexity has also accelerated digital transformation, enabling businesses to offer more efficient services by making data-driven decisions and simplifying transactions.

Despite their benefits, the complexity and ubiquity of current IS pose significant challenges. *Personal Data Protection* (PDP) has gained prominence as data collection and sharing continue to expand. To protect individuals' privacy, laws and regulations like *the General Data Protection Regulation* (GDPR) [1] have been established, while frameworks supporting data exchange aim to strike a balance between privacy and the benefits of data sharing. Interoperability among systems and technologies is also essential for this purpose. Therefore, developing robust *Enterprise Systems Architectures* (ESA) that address these challenges is essential to support the needs of businesses and individuals. ESA becomes crucial in identifying the types of data being processed, as well as the data domain and subdomain owners within organizations, assessing associated risks, and efficiently managing regulatory requirements and data subject demands to avoid penalties and compensations.

This paper proposes a method to support PDP based on the use of *i** notation, focusing on how dependencies can track owners responsible of specific data, and system components used for its processing (legally known as data treatment). The DHARMA-PDP method proposed in this paper, assists Data Protection Officers in timely fulfilling regulatory requirements and obligations.

The document is structured as follows: Section 2 provides background information and related work, section 3 presents the case study, section 4 presents the method and how it may support the analysis for PDP compliance, and finally, section 5 presents conclusions and future work.

The 16th International iStar Workshop, September 03–04, 2023, Hannover, Germany

jackeline.fernandez@cedia.org.ec (J. Fernandez); carolina.sacoto@cedia.org.ec (C. Sacoto); karina.abadr@cedia.org.ec (K. Abad); jpcarvallo@cedia.org.ec (J.P. Carvallo)

0009-0003-7575-1394 (J. Fernandez); 0000-0002-8999-8947 (C. Sacoto); 0000-0003-2173-6079 (K. Abad); 0000-0001-6678-4774 (J.P. Carvallo)

2. Background and Related Work

Organizations face significant challenges in correctly applying complex legal provisions for personal data protection, especially with constant changes in processes, employees, services, and technological platforms [8][9]. Challenges include updating data processing records, implementing technical and organizational measures, and responding efficiently to data subject requests [10], all while facing resource and capability limitations for compliance [11]. To address these issues, organizations need methods and management systems that facilitate regulatory compliance [12], enabling structured and documented processes to ensure proper application of personal data protection regulations and timely compliance with regulatory requirements and data subject demands [13][14].

Various methods and approaches, like Privacy by Design (PbD) [15], Data Protection Impact Assessment (DPIA) [16][17], ISO 27001 [18], COBIT (Control Objectives for Information and Related Technologies) [19], and the NIST Privacy Framework [20], contribute to data protection compliance, though not designed specifically for it. Despite these tools, efficiently addressing compliance remains challenging, as existing methodologies focus exclusively on technical, process-oriented, or legal approaches, overlooking the need for a multidisciplinary team with technical, process, and legal expertise for comprehensive compliance [22][23].

Previous research in software engineering emphasizes the importance of integrating data protection principles into early stages of software development [24][25][26]. However, translating these principles into requirements engineering activities remains challenging [27]. The lack of models, processes, and tools supporting privacy by design throughout the software development life cycle, especially concerning the requirements of the General Data Protection Regulation (GDPR), has been identified as a critical issue [27].

To facilitate compliance with data protection regulations in requirements engineering, interdisciplinary collaboration between software engineers and legal experts has been a solution, but it can be expensive and time-consuming [21]. In response, this paper proposes a collaborative method based on *i** notation and the DHARMA method [2]. The DHARMA method, extended with activities specifically engineered to support PDP, encourages active participation of non-technical stakeholders [3][4][5][6][7]. This approach translates legal obligations into technical requirements, empowering software engineers, promoting collaboration between legal experts and engineers, and involving stakeholders throughout the organization. The resulting method aims to ensure comprehensive compliance with data protection regulations, assisting organizations in safeguarding privacy and data security in the ever-evolving digital landscape.

3. Case Study

CEDIA (*Corporación Ecuatoriana para el Desarrollo de la Investigación y Academia*) is a non-profit organization that has been at the forefront of promoting the development of research and academic activities in Ecuador since its inception. Established with the vision to foster a collaborative network among Ecuadorian universities and research institutions, CEDIA has been instrumental in driving technological innovation and academic excellence in the country.

CEDIA's primary objective is to facilitate the sharing of knowledge and resources among its member institutions, thereby enhancing the quality of education and research in Ecuador. It achieves this by providing advanced network infrastructure, promoting collaborative research projects, and offering a range of services such as cloud computing, digital repositories, and e-learning platforms.

In an era where data is a valuable asset, CEDIA recognizes the importance of data protection and privacy. As an organization that manages a significant amount of personal data, it is imperative for CEDIA to ensure the highest standards of data protection. This is not only a legal requirement under the Ecuadorian Personal Data Protection Law enacted in 2021, but also a moral obligation to respect the privacy rights of individuals.

Implementing data protection measures is crucial for CEDIA for several reasons. Firstly, it helps to maintain the trust of its member institutions and the public. Secondly, it helps to prevent potential legal and financial penalties that could result from non-compliance with PDP law. Lastly, it contributes to the overall goal of creating a safe and secure digital environment for education and research in Ecuador and sets a positive example for other organizations in the country.

4. Method

The complexity PDP analysis for compliance with regulations, commands advanced knowledge in several fields, including technology, information systems, data analytics, governance, and personal data protection law. Given this complexity, the proposed method mandates the establishment of a multidisciplinary team of professionals. This team should comprise representatives from each organizational area, possessing a thorough understanding of the processes within their respective domains. For a holistic approach to PDP compliance, the team should also include at least one information security technician and a legal professional well-versed in data protection regulations. Their expertise will underscore the crucial aspects related to legal compliance.

Structure of CEDIA's team included 18 professionals from 11 areas of the organization. 7 systems engineers, 6 lawyers, 2 business administrators, a communicator, an accountant and a psychologist. 4 were managers, 2 mid-managers and the remaining operational personnel. In addition, external advice was provided by two lawyers and a systems engineer certified in information security and implementation of ISO 27001 and ISO 27701.

To equip the team with the necessary skills and knowledge, basic training shall be provided in data management, personal data protection regulations, and *i** notation. In the case of CEDIA, training was completed with guidelines based on the lessons presented in [4][7], ensuring a comprehensive understanding of the subject matter.

To guide the process in a systematic way, the method proposes the use the four activities in the DHARMA method [2] as basic steps. This method aims to the definition of Enterprise Systems Architectures (ESA) using the *i** notation. The theoretical bases to support the method in the analysis of enterprise context, structure and strategy, are two models defined by Porter's models of the market forces and value chain [28]. The activities in the DHARMA method are:

- **Activity 1. Modelling the enterprise context:** The organization and its strategy are analyzed to identify its role within the context, defining *Context Actors* (CA) in relation to marked forces and *Organizational Areas* (OA) in relation to value chain primary and supporting activities. At the end of this activity *i** SD models are built, to describe the *context and scope of the organization* (CM).
- **Activity 2. Modelling the environment of the system:** In this activity, the impact of a system-to-be is analyzed by identifying dependencies in CM, that can be partially or fully satisfied (automated) by system services. The result is an *i** SD model representing the system's ability to fulfill dependencies related to different CAs or OAs.
- **Activity 3. Decomposition of system goals:** Dependencies included in the CM are analyzed and decomposed into a hierarchy of intentional elements required to satisfy them. These elements depict the services that the system must provide (functional requirements) as well as restrictions on them (non-functional requirements). An *i** SR diagram for the system is built.
- **Activity 4. Identification of system architecture:** This activity includes the identification of System Actors (SA), which represent atomic software domains. Intentional elements identified in Activity 3 are analyzed and semantically grouped. Each aggrupation reveals the services that are expected to be provided by SA structuring them.

The assessment identified a total of 178 CA and 11 OA and 2119 dependencies, see Table 1 for some indicators in relation to resulting CM. 112 processes are required for the provision of the 64 services included in CEDIAS service package. 116 software tools (SA) integrate CEDIA's ESA and are used for their provision. Due to the magnitude of the model, a tabular representation was adopted following the guidelines presented in [7] (see table 2 for an excerpt).

Table 1
Summary of the numbers obtained in the study

OA	Dependencies			Actors		Software Components	Processes	Dependencies with Personal Data
	Goal	Quality	Resource	OA	CA			
ICT	803	46	100	10	13	54	15	60
Innovation	150	5	137	9	14	8	36	170
Education	78	0	86	7	6	8	3	148
Digital Printing	7	0	7	10	6	3	6	15
Legal	29	0	35	10	11	5	8	62
Strategic Planning	21	0	10	10	6	8	6	28
Marketing & Communication	20	0	29	10	3	10	4	83
Sales	14	0	13	3	2	4	2	21
PMO	121	5	125	7	8	6	13	86
Finances & Administration	69	0	58	10	10	5	9	114
Human Resources	53	2	96	10	3	5	10	128
TOTAL	**1365**	**58**	**696**	**96**	**82**	**116**	**112**	**915**

The activities of the method allow for the systematic and precise identification of CAs, OAs, SA and intentional elements e.g., dependencies, and establishes the "ideal" ESA and its services as basis for PDP analysis. However, additional steps are required to complete PDP compliance process. Method got extended with 5 additional activities in a framework called DHARMA-PDP:

- **Activity 5. Reverse mapping of existing systems:** This activity can be applied in forward or reverse engineering. In the first case ESA describes the requirements of the system-to-be and the software components needed for its implementation, those to be acquired (e.g., FOOS, COTS or Services) and those to be built from the scratch. In the second case, when ESA is already implemented and multiple software components are up and running, a reverse engineering mapping is required to relate system components in operation to SA and their expected services. This helps to identify unimplemented, unnecessary, or augmentable services in relation to ESA. Additionally, it entails identifying new requirements for software components integration and, analyzing and optimizing personal data shared among them. As an example, in the case of CEDIA, the analysis proved that some software components, namely *ERP* and *Management* SA, used in 34 and 54 out of the 112 processes accounted in table 1, required significant improvements on their integration.
- **Activity 6. Analysis of data associated to dependencies:** Activity 6 involves a thorough analysis of each identified dependency included in CM, to determine the specific data associated with them, particularly personal data. In typical ESA implementation cases, UML use cases and class diagrams can be used for this task. However, in CEDIA's case, since ESA was already implemented, representatives from OA and other project team experts examined system interfaces and processes to identify the data treated, particularly personal information. A total of 915 dependencies were identified treating personal and sensitive data (see Table 1). Table 2 provides an excerpt of personal data associated with certain dependencies in CM.
- **Activity 7. Data protection categorization:** This activity involves data protection categorization, where identified data types are mapped to corresponding categories defined in the PDP law applicable in the territory. In the case of Ecuador, these categories include personal identification, special categories (e.g., sensitive, data of children and adolescents, persons with disabilities, credit-related), personal characteristics, social status, academic and professional, employment, and economic, financial, and insurance data. A total of 106 out of 915 dependencies identified in activity 6 were marked critical in this activity.
- **Activity 8. Risk and impact analysis:** Following with the method, activity 8 involves conducting a qualitative risk analysis to assess the potential impact on the organization, considering the PDP Law applicable in the territory. This analysis identifies threats, vulnerabilities, impact, and likelihood of occurrence.

  Qualitative risk analysis at CEDIA showed that, 23 out of 106 dependencies identified in activity 7, required a *Data Protection Impact Assessment* (DPIA). The DPIA analyzed data related to dependencies in relation to a checklist containing 44 risks, 20 security, 20 legal, and 4 international data transfer. The checklist was constructed considering the risks suggested in

standards and legal bodies such as ISO 27001, 27702 and GDPR. Figure 1 shows the risk map resulting from the activity. Data associated to a dependency can be subject to multiple risks.

- **Activity 9. Mitigation strategy definition:** Finally, mitigation strategies must be defined for each of the risks falling outside an acceptable threshold, starting for the most critical ones. These strategies shall be designed to reduce the impact or likelihood of the risks, thereby enhancing the organization's data protection posture. In CEDIA's case, controls have also been selected from those suggested by ISO 27001, ISO 27701, and GDPR, according to the corresponding data processing activities. For instance, measures in relation to personal data associated to dependencies in the occupational health and safety field included, the establishment of a consent document allowing the process of health data and the definition of time limits for periods for which data had to be preserved. The dependencies of CEDIA's core areas (e.g., ICT) were given priority over others less critical such as Digital Printing.

5. Conclusions and Future Work

The study presented in this paper has demonstrated the application of the *i** notation to support Personal Data Protection compliance. The proposal makes use of the DHARMA-PDP method, which allows for a systematic and precise identification of Context Actors, Organizational Areas, intentional elements (e.g., dependencies) and System Actors, structuring the "ideal" Enterprise Systems Architecture (ESA) and its services. However, the benefits go far beyond this scope. DHARMA-PDP also help Data Protection Officers in fulfilling data subjects' requirements and meeting regulatory obligations, identifying personal data, categorizing risks associated to them and analyzing mitigation strategies, required to comply with existing regulations and implement best practices to protect personal data.

It is acknowledged that there are some threats to validity in this study. One of the main threats is the potential for bias in the qualitative risk analysis conducted in activity 8. This analysis relies on the expertise and judgement of the individuals conducting the assessment. Additionally, the study is limited to the context of CEDIA and Ecuador, and may not be generalizable to other organizations or contexts.

However, based in the results of this study, the DHARMA-PDP method has shown its potential in supporting organizations to ensure compliance with existing regulations and implement best practices to protect personal data. Future work will focus on refining the method and expanding its application to other contexts to further validate its effectiveness.

Table 2

Example of Personal Data associated to dependencies in CM.

Actor 1	Actor 2	Dependency	Type	Direc-tion	Process	Responsible	Personal Data
Human Resources	National Institute of Social Security	Entry notice	Resource	>	PA4-1 Staff Admition	HR	Name, last name, date of birth, DNI, disability
Human Resources	Ministry of Labor	Payroll	Resource	<	PA4-3 Payroll Management	HR,	DNI, Name, Last name and salary
Finances & Administration	Internal Revenue Service	Tax annex	Resource	>	PA3-1 Purchase Management	Finances & Administration	DNI, Name, Last name, salary and signature

Probability / Impact	Very Low	Low	Medium	High	Very High
Very High	1	7	25	21	0
High	1	24	106	86	0
Medium	0	45	101	18	0
Low	5	92	225	145	1
Very Low	32	371	844	323	12

Figure 1: Risk map for CEDIAS PDP process

References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
[2] Carvallo, J.P., Franch, X. On the Use of *i** for Architecting Hybrid Systems: A Method and an Evaluation Report. Proceedings of PoEM 2009.
[3] Carvallo, J. P., Franch, X. Building Strategic Enterprise Context Models with *i**: A Pattern-Based Approach. Proceedings of TEAR 2012.
[4] Carvallo, J.P., Franch, X. Lessons Learned on the use of *i** by Non-Technical Users. iStar 2014.
[5] Abad, K., Carvallo, J.P., Peña, C. iStar in Practice: On the identification of reusable SD Context Models Elements. Proceedings of iStar 2015.
[6] Abad, K., Pérez, W., Carvallo, J. P., Franch, X. *i** in Practice: Identifying Frequent Problems in its Application. Proceedings of ACM SAC 2017.
[7] Carvallo, J.P., Franch, X.: An empirical study on the use of *i** by non-technical stakeholders: the case of strategic dependency diagrams. Requirements Engineering Journal. Vol. 24, pp.27–53 (2019).
[8] S. Sirur, J. RC. Nurse, and H. Webb. "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)". Proceedings of MPS 2018.
[9] M. Smith and J. Palmer. "ANALYSIS: Three Years Later, GDPR Compliance Still a Challenge". https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-three-years-later-gdpr-compliance-still-a-challeng . (2021).
[10] M. Saltarella, G. Desolda, R. Lanzilotti, "Privacy Design Strategies and the GDPR: A Systematic Literature Review", HCI for Cybersecurity, Privacy and Trust, vol.12788, pp.241, (2021).
[11] M. Bańka, et. Al., "Practical Methods of Implementation for the Indispensable Mechanism of GDPR Compliance", Wroclaw Review of Law, Administration & Economics, vol.0, no.0, (2022).
[12] D.F. Martínez-Martínez. "Unification of personal data protection in the European Union: Challenges and implications". Profesional De La información, 27(1), 185–194. (2018).
[13] Y. -S. Martin, A. Kung, "Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering,". Proceedings of EuroS&PW 2018.
[14] C. Lambrinoudakis. "The General Data Protection Regulation (GDPR) Era: Ten Steps for Compliance of Data Processors and Data Controllers". Proceedings of TrustBus 2018.
[15] B. Mashaly, S. Selim, A. H. Yousef, K. M. Fouad, "Privacy by Design: A Microservices-Based Software Architecture Approach". Proceedings of MIUCC 2022.
[16] Party, Data Protection Working. "Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP29). Artic. 29 Data Prot. Work. Party. WP 248 rev 22 (2017).
[17] Wright, David, et al. "Integrating privacy impact assessment in risk management." International Data Privacy Law 4.2 (2014), pp155-170.
[18] I. M. Lopes, T. Guarda and P. Oliveira, "How ISO 27001 Can Help Achieve GDPR Compliance,". Proceedings of CISTI 2019.
[19] VM. Orrego. "La gestión en la seguridad de la información según Cobit, Itil e Iso 27000." Revista Pensamiento Americano 4.6 (2013): 21-23.
[20] J.S. Hiller, R.S. Russell. "Privacy in crises: The NIST privacy framework." Journal of Contingencies and Crisis Management 25.1 (2017): 31-38.
[21] F. Ciclosi, F. Massacci. "The Data Protection Officer: A Ubiquitous Role That No One Really Knows", IEEE Security & Privacy, vol.21, no.1, pp.66-77, 2023.
[22] J. Fernandes, C. Machado, L. Amaral. "Identifying critical success factors for the General Data Protection Regulation implementation in higher education institutions", Digital Policy, Regulation and Governance, Vol. 24 No. 4, pp. 355-379. (2022).
[23] A. Tsohou, M. Magkos, H. Mouratidis, G. Chrysoloras, L. Piras, M. Pavlidis, J. Debussche, M. Rotoloni, B. Gallego-Nicasio Crespo, "Privacy, Security, Legal and Technology Acceptance Requirements for a GDPR Compliance Platform", Computer Security, vol.11980, pp.204, 2020.
[24] Sartoli, S. Ghanavati and A. Siami Namin, "Towards Variability- Aware Legal-GRL Framework for Modeling Compliance Requirements,". Proceedings of ESPRE 2020,.
[25] S. Ghanavati, A. Rifaut, E. Dubois and D. Amyot, "Goal-oriented compliance with multiple regulations," Proceedings of RE 2014.
[26] A. Siena, A. Perini, A. Susi and J. Mylopoulos, "Towards a framework for law-compliant software requirements". Proceedings of ICSE 2009.
[27] V. Camargo, et. Al. Privacy by Design and Software Engineering: A Systematic Literature Review. Proceedings of SBQS '22.
[28] M. Porter, "Competitive Strategy". Free Press, New York, NY, United States, 1980.