Towards the integration of the GDPR in the Unified Software Development Process

Elena Gómez-Martínez, Miguel Marroyo, Silvia T. Acuña
Departamento de Ingeniería Informática
Universidad Autónoma de Madrid, Madrid, Spain
{MariaElena.Gomez, Miguel.Marroyo, Silvia.Acunna}@uam.es

***Abstract*—The General Data Protection Regulation (GDPR) is the core of digital privacy legislation across Europe (EU), and it applies to processing carried out by organisations operating within and outside the EU that offer goods or services to individuals in the EU, including software products. Nevertheless, software teams are generally unaware of the legal requirements for personal data protection and its application throughout the software life cycle. In this paper, we propose a comprehensive guidance to integrate compliance with GDPR requirements within the Unified Software Development Process (UP) across the entire lifetime.**

Keywords-data protection regulation; unified software development process; personal data; privacy requirements.

I. INTRODUCTION

As part of the software process activities, software engineers should get acquainted with and understand guidelines related to information privacy, as software requirements should comply with data privacy laws. Therefore, development team members need to be familiar with the applicable personal data protection legislation [12]. In addition, the identification of the privacy requirements, that is, the protection of personal data that are processed by complex systems, is a tough, error-prone task in social networks where users often enter personal and other sensitive data that would otherwise be subject to varying levels of personal data protection, security and privacy [25].

The European Union (EU) General Data Protection Regulation 2016/679 (GDPR) comes into force in May 2018 [13], representing an advance in personal data protection. For enterprises in the EU or those that work with resident data in it, this regulation means a new challenge, namely, to avoid costly fines (up to 20 million or 4% of turnover) and offer their clients a service that guarantees their privacy rights. Not only should software engineers validate that installed systems comply with privacy requirements, personal data and data protection needs should also be identified during the early development activities, including requirements capture and analysis, in order to specify the associated requirements [12][19][9]. For instance, the personal data gathered from users by developers designing a medical data management application, where age or sex are important, will not be the same as for a library management system, where such data are unnecessary. If these data and needs are identified later during the development process, it will be more costly to solve data privacy-related problems, because the changes that have to be made to the future system will tend to affect more functionalities [3][18][22]. Nevertheless, the software development teams do not have a framework for adopting the personal data protection legislation in software development, as the this legislation should change development team work methods by, for example, adopting a series of features and controls related to consent, documentation and privacy responsibilities throughout the software development process [4][5][26].

Regarding the lack of a framework for adopting the personal data protection legislation in software development, in 2017, in a survey conducted by PwC [23], 92% of organizations in the United States of America believe that even though GDPR is a European regulation, it still affects their business and therefore compliance should be a priority. In the same year, Deloitte conducted a survey of organizations in EMEA (Europe, Middle East and Africa) [11], in which only 15% of companies believed that they could fully comply with regulations by May 2018. Companies like Facebook or Google have been fined US$114 million, and countries such as Greece, Portugal or Slovenia have not adjusted their measures to adapt to their national regulations [14]. Therefore, despite the importance of GDPR has been recognized, due to the lack of a defined framework to incorporate GDPR into the software development process, it is difficult to fully take action to comply with the legislation.

The objective of this article is to provide a framework from the point of view of software engineering that incorporates the European General Data Protection Regulation in the Unified Software Development Process or Unified Process (UP), thereby software teams can define and specify the privacy requirements in early development activities and throughout the software development process, including design, implementation, testing, and maintenance.

The research question is if: it is feasible to apply the GDPR into the UP. GDPR [13] has important value in the technical and information technology fields at European and international levels, so GDPR must be considered in any process related to software development. In addition, it guarantees that if you follow its instructions, the processing of personal data will be transparent, honest, and safe, which is very important for companies and organizations as well as users themselves. The Unified Process [17] has been selected thereby that it can be tailored to a wide range of software development projects and provides a formalised prescription of the entire software development process, as it specifies all the software process modelling elements through Unified Modelling Language (UML) [21]. The research method used consists of the analysis and synthesis of the GDPR and its justified inclusion in the UP following the standard set by the Data Management Association (DAMA) International, known for its data management guide [10]. To verify this adaptation, the Regulatory Compliance List developed by the Spanish Agency for Data Protection (in Spanish, *Agencia Española de*

DOI reference number: 10.18293/SEKE2021-069

Protección de Datos, AEPD) [2] was used, which allows us to approximate in hindsight compliance percentage that would be achieved following our proposal. All this work has been carried out by a team of software engineers together with a legal advisor expert in personal data protection and data auditing. Our main contribution is to provide comprehensive guidance to familiarize a development team with the legal requirements of the regulations throughout all the software development activities from requirements elicitation to deployment to the customer and maintenance. This solves the problem of validating compliance with the law a priori and not just compliance in hindsight when the system is already in use.

The rest of this paper is organized as follows. Section II introduces key basic concepts. Section III presents our approach to integrate the GDPR in the Unified Process. Section IV compares with related approaches. Finally, Section V outlines the conclusions and future work.

II. Background

A. Legal Environment: GDPR and LOPD

The GDPR [13] is the core of Europe's digital privacy legislation and gives back control over personal data to citizens far more than its predecessor the Data Protection Directive or Directive 95/46/EC. It applies to organisations in all member states across Europe, including any organisation outside of the EU which offer goods or services to customers or businesses there. The GDPR provides the following rights for individuals: a) **The right to be informed**, Articles 13 and 14 of the GDPR specify that individuals have the right to be informed about the collection and use of their personal data; b) **The right of access**, individuals have the right to access their personal data; c) **The right to rectification**, under Article 16 each individual has the right to have inaccurate personal data rectified; d) **The right to erasure**, under Article 17 each individual has the right to have personal data erased; e) **The right to restrict processing**, Article 18 gives individuals the right to restrict the processing of their personal data in certain circumstances; f) **The right to data portability**, individuals has the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format; g) **The right to object**, Article 21 gives individuals the right to object to the processing of their personal data at any time; h) **Rights in relation to automated decision making and profiling**, Article 22 has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

The directive entered into force on 5 May 2016 and EU countries had to transpose it into their national regulations. The Law on the Protection of Personal Data and Guarantee of Digital Rights (in Spanish, *Ley de Protección de Datos Personales y Garantías de los Derechos Digitales*, in short LOPD) [7] sets out the data protection framework in Spain, alongside the GDPR. Despite having some dissimilarities with respect to the GDPR, they do not impact the software development. Therefore, both acronyms, LOPD and GPDR, will be used interchangeably in this paper, employing the latter for the sake of brevity. We focus on UP process workflows (activities) and all the software development process activities that will be taken into account when analysing the Spanish LOPD: requirements, analysis, design, implementation, test and maintenance.

B. Data Management Book of Knowledge

The guidebook named "*The DAMA Guide to the Data Management Body of Knowledge*" (DAMA-DMBOK) [10] establishes a framework to data management standards and practices for data management, remarking the importance of data quality and ethics. This framework is structured around the 11 Knowledge Areas with core activities surrounded by software lifecycle and usage activities, contained within the structures of governance. Settled within the Knowledge Areas are the essential objectives and principles of data management. Here we only focus on those related to the software process.

Data Governance provides the general template and oversight to govern data management by establishing a framework of decision rights over data that accounts for the company's needs, and according to the current legislation. It affects to all the software lifecycle encompassing from the access policy, usage, security and quality to the fulfilment of requirements. **Data Architecture** defines the master plan to handle and maintain data assets by with regards to organizational strategy which are already establish with other strategic data requirements and designs to meet these necessities. **Data Modelling and Design** determines, analyses, represents, and communicates data requirements in a detailed form which is called the data model. **Data Storage and Operations** comprises the design, application, and maintains of stored data to make the most of its value. **Data Security** ensures that data privacy and confidentiality are maintained that data is accessed appropriately and not breached across various channels of use. **Data Integration and Interoperability** includes processes associated with the movement and consolidation of data within and between data stores, applications, and organizations. **Document and Content Management** are measures and strategies which are used to handle the lifecycle of data and information found in a range of unstructured media, especially documents needed to support legal, regulatory compliance requirements and ethics implication. **Data Quality** includes the planning and implementation of quality management techniques to measure, assess, and improve the fitness of data for use within an organization.

III. Integrating the GDPR

The Spanish LOPD [7] is comprised by 97 articles. Many of them are transversal to the activities of the software development process, and therefore they can be affected. Notwithstanding, not all the articles have a place within any of the activities given its purely legal nature and that it does not apply to the technological context. Several articles in the LOPD mention crucial information contained in the GDPR. In those cases, we have contemplated that information. We will refer as (Art. X) to the Article labelled X of the LOPD.

A. Procedure

Before analysing the GDPR, we have firstly established a correspondence of each Knowledge Area of DAMA-DMBOK with the UP activities in order to guarantee the data management. Note that not all Knowledge Areas have been considered

since they are not included in the UP. This correspondence is summarised in Table TABLE *I*. As it can be observed, data management process and governance are considered globally strategic to the entire software lifecycle. In addition, data security shall affect all the process, otherwise security could be uncompleted, since it is designed, but not implemented. Processes related to architecture, modelling, design, storage and operations belong to design activity of the UP, which considers all the software requirements. Data ethics and management are closely related to the fulfilment of users' rights; therefore, they correspond to the analysis activity. Since these rights have to be guarantee during all the software lifecycle, we have included it in the maintenance activity. To integrate the legal requirements imposed by the GDPR into the UP [18], we propose a procedure with the following steps:

1. Overview of the regulation: Initial reading of every article and extraction of keywords and concepts which can guide us to correlate UP activities within the GDPR.
2. Reading of each article: Each article is analysed in detail by focusing on a set of keywords in Table TABLE *I* and Knowledge Areas of DAMA-DMBOK. After this study, we determined if the article can be applicable to any development activity.
3. In the case the article is applicable, we placed it in one or more development phases, and extracted new keyword if needed and reassessed the examined articles.
4. Otherwise, we evaluated the next article.

The inclusion of the GDPR into the UP has been carried out by an interdisciplinary team composed by senior and junior software engineers together with an expert in data protection and data auditing. For the sake of brevity, additional documents are available at https://github.com/egomez26/SEKE2021.

B. *Requirements and Analysis*

Since most of the legal requirements are in the initial phases of the project, we have decided to tackle both activities at the same time. All the activities to carry out during this phase are summarised in the workflow in Fig. 1, whose rationale is described below.

TABLE I. KEYWORDS TO IDENTIFY SOFTWARE ACTIVITIES IN EACH ARTICLE

Elicitation & Analysis	**Design**	**Implementation & Testing**	**Maintenance**
Rights and Obligations	Storage	User	Lifetime
Data type	Transfer	Validation	Data life cycle
Purpose	Architecture	Interface	Register
Requirements	Security	Consent	Security
Processing	Interface	Communication Provide information	Control
Limitations	Communication Provide information	Rights and Obligations	
Assessment	Measures and codes Controller Data access	Security	

In the early activity of any software development, the data scope is defined, that is, their data type and purpose. According to (Art. 4), data have to be precise and represent the reality. Furthermore, it is mandatory that users express their explicit consent to use their required personal data and the purposes of the processing, and to be informed of this fact (Art. 8). Therefore, we need to identify the minimum information with personal data for our application and to not use this information for any kind of discrimination on the grounds of age, sex, gender and sexual orientation, race or ethnic group, political convictions, health, biometric information, and/or religion (Art. 9). Notwithstanding, there exist exceptions to use the aforementioned data if individual gives her consent or that the data processing is vital in a legal process (Art. 10).

Concerning the purposes of data processing, once the data are collected, the user has the legal right to claim this purpose at any time, requiring the name of the contact detail of the organization, identity of the data protection officer, the lawful basis of the processing, and any related information (Art. 15 to 22), including data categories and their sources (Art. 11). The Spanish LOPD also encompasses the following data processing to protect personality or habits aspects, automated individual decision-making, systematic profiling, monitoring or geolocating of people, genetic information, vulnerable people or at risk of social exclusion, and/or preventing nor discouraging from exercising their rights. In all these cases, the application will have to require the user's acceptance or her legal representative (Art. 12). Obviously, the application has to guarantee all their rights of end-users, and the security tools to achieve it (Art. 80). Therefore, the main functionalities of the software must be considered if this information is processed, e.g., application for banking or video surveillance. We must also define the kind of application, target end-users, processed information, context of use, and derived contents (Art. 87). In the following, we describe the most sensitive applications. In the working environment, since service providers may be a natural person or a corporate entity, information related to self-employed, freelances, individual entrepreneurs and professionals has special attention (Art. 19). In these cases, we will only consider the minimum personal data to locate her professional activity, such as working address and phone number. We must also contemplate the direct or indirect geolocation of workers (Art. 90) or video surveillance at workplaces (Art.

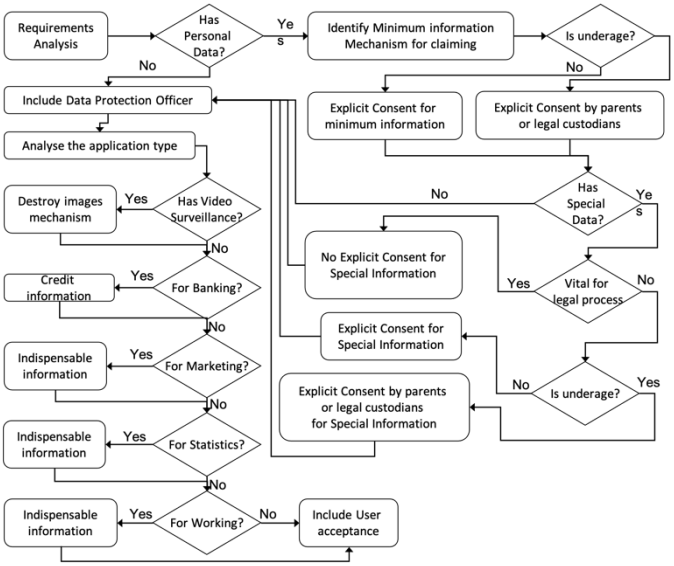

Figure 1. Activities in the Analysis Phase

89). If we are developing a banking application, it is lawful to have credit information if that data has been provided by the creditor (Art. 20). It is also lawful when they derived from the development of a commercial transaction, i.e., when the company structure has been modified, acquired or sold (Art. 21). Video surveillance applications can process captured images and videos if the purpose is to guarantee safety of individuals and facilities (Art. 22). Thus, a mechanism to destroy these images or videos in a month from their acquisition must be considered. Marketing communication applications must create an information system to store the indispensable data for those individuals who do not want to receive these communications (Art. 23). Statistical applications can use personal data at the prior disposal of those affected, provided voluntarily (Art. 25). Applications involving underage users, we need to storage the consent of their parents or legal custodians to process their information in the analysis activity (Art. 92). Data controllers, processors and officers play a key role in software applications, since we must contemplate them their different responsibilities, role access and functionalities in our system (Art. 28 to 37). A data controller can handle personal data using technical measures to guarantee that the Directive is fulfilled. They are in charge of registering all the processing activities (Art. 28). Data officers are able to lock information (Art. 32). In addition, the application must provide default functionality to erase personal data for individuals who exercise their right to be forgotten (Art. 94), to modify inaccurate or low-quality information (Art. 93), and to port personal data (Art. 95). To guarantee digital security, we will need to analyse it in this phase, considering level of confidentiality for sensitive data, involved roles, administration procedures, maintenance plans, monitoring, auditing and policy compliance (Art. 82), that we will describe in the following sections.

C. Design

Design activities define the data domain and the architecture from those requirements obtained in the previous analysis. One key aspect during design is to guarantee confidentiality in data structures, interfaces and algorithms (Art. 5). With this purpose, the application ensures not authorized data processing, and lost or destruction of personal data. In addition, data must be accurate and, if needed, updated (Art. 4). Designers must take into account all these aspects to prepare databases, including memory requirements, index and precise processing to make queries, generate verified statistics, provide backup services and balance to allow the access at any time. Remark that it is not possible to process data categories into conflict with Art. 9, that is special information, and criminal records (Art. 10). We will also include in databases information such as identification of the data processing officer, if there are data of special categories, and data sources (Art. 11). Software systems must also consider mechanisms to register all the activities related to Art. 31. This register must contain the following fields: name and contact details of the data processing officer, purpose of processing, categories of personal data and person concerned, categories of recipient of those personal data, transaction to third countries or international organizations Art. 82, expected timeframe for removing data, technical and organizational measures to guarantee data security. This register shall have a relation N:N between the Register class and each data category. As a step forward, to facilitate the integration of the legal requirements into design activities, we have also drawn a representation of the GPDR. With this aim, we use MDE (Model Driven Engineering) [8] to formally define the syntax. Models are described using a modelling language (e.g., UML), whose syntax is defined through a meta-model. Particularly, we represent the GDPR as a DSL (Domain Specific Language) [16], an excerpt depicted in Fig. 2. This DSL can be applied to any application domain.

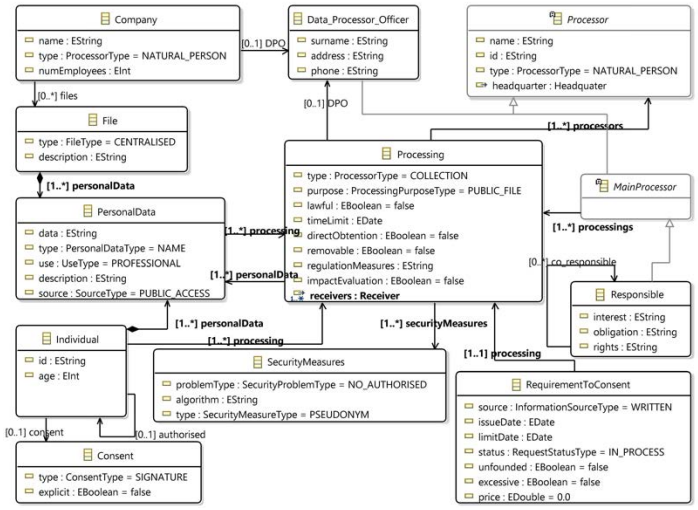

Figure 2. Excerpt of the Domain Specific Language for the Design Phase

D. Implementation and Testing

During these activities, the design is translated into code and the tests are performed to validate and verify that the implementation is valid according to the requirements. From the GDPR viewpoint, those activities are straightforward to carry out, since legal requirements have been already fulfilled at early stages. Fig. 3 illustrates all the activities involved in these phases. The implementation shall develop user interfaces displaying users' rights and collecting their explicit consent, which shall be expressed voluntarily, specifically, and unambiguity by means of a clear affirmative action (Art. 6). For instance, it could be implemented using a pop-up window with this information. It is noteworthy that in no case the user consent can be marked as accepted by default (Art. 90). That is, if there is a checkbox for the acceptance, its default value must be unchecked. There are other means of obtaining the user consent, such as digital certificates, electronic signatures, or electronic national ID issued by

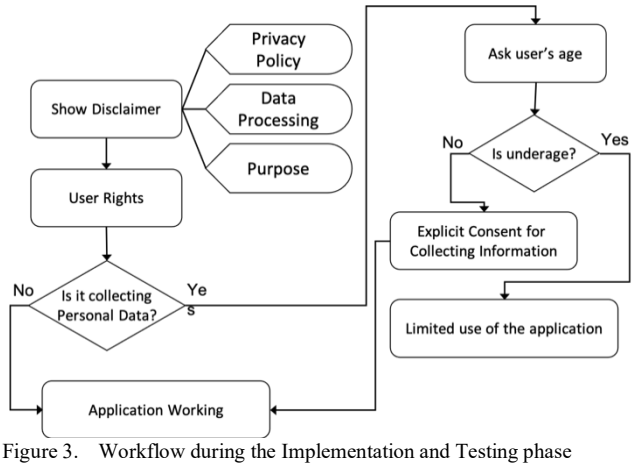

Figure 3. Workflow during the Implementation and Testing phase

certification authorities. As mentioned in analysis activities, the user interface shall validate user's age. The processing of data of a child under fourteen shall be lawful only if it has the consent of their legal custodians, so it will be necessary to collect somehow such consent (Art. 7). In the case of not obtaining this consent, the application may have a restricted functionality. As a general rule, the application or website shall include a disclaimer reporting its owner, the privacy policy on which the following is communicated: the data processing, its purpose, if you have recipients and the identity and address of the person responsible for the treatment. Finally, it shall display the rights of the user and, if necessary, the cookie policy if they are used.

E. Maintenance

Once the product is delivered to the customer, the next activity is maintenance, which will be carried out by either the development company or a software maintenance company. In this activity. The activities carried out during this phase are summarised in Fig. 4. The European GDPR does not apply to the processing of personal data of deceased persons or of legal persons, therefore they must be removed. Nevertheless, the Spanish LOPD authorises to exercise the rights to access, of rectification and erasure with respect to the personal data of deceased persons to relatives and their legal successors (*Art. 3*). The role of the data controller will participate in case it is necessary to block those personal data (*Art. 32*). In the event this unlocking does not occur, the data controller will eventually have to destroy the personal data. Moreover, the data controller will be in charge of registering all those activities occurring on the data *(Art. 31)*, in order to reliably monitor that they are correctly processed in the event that such information is requested. One of the key issue of data quality is accuracy, that is, personal data will be exact and, if necessary, updated (*Art. 5*). During the maintenance, the software product must carry out tasks to validate these premises, including the automatic erasure of personal data once the limit time has reached, periodic updating the information and revision of invalid data, uncompleted or void.

IV. Related Work

We reviewed the literature in search of recent related work on the scope of privacy requirements definition and management in software process activities. The goal of the literature search was to the answer the following question: How are the articles of the European GDPR adopted in the software development process? From the analysis of the selected studies, we classified the related work into two categories depending on the type of software process activity addressing data privacy issues:

- Adoption of the GDPR in early development activities, like requirements elicitation, analysis and specification, and software design. This addresses the problem of validating compliance with the regulation a priori before starting and during software system development.
- Adoption of the GDPR in later development activities, such as system testing and maintenance. This addresses the problem of validating compliance with the regulation when the software system is in use.

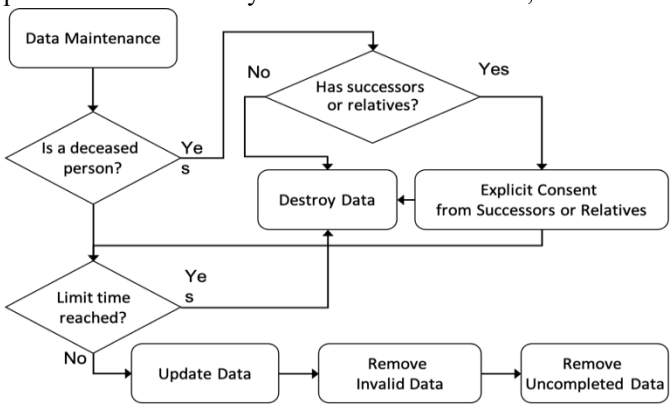

Figure 4. Workflow during the data maintenance

With respect to papers dealing with GDPR issues in early development activities, Meis and Heisel [19] report a systematic extension of the problem-based privacy analysis method (ProPAn) designed to identify software system privacy needs based on a set of functional requirements. Based on studies published from 2009 to 2019, Dias et al. [12] reported a systematic literature review (SLR) on software privacy and privacy requirements and the methodologies and techniques that are used for their elicitation and specification. The methodologies include LINDDUN, SQUARE for Privacy, and PriS, among others. The SLR results revealed that ICT practitioners are not altogether familiar with software privacy, privacy requirements and the Brazilian LGPD, which is an obstacle to the application of laws and directives governing data privacy. Amorim et al. [3] suggest the use of gamification techniques as an option for providing practitioners at an organization with data privacy training. Mavroeidi et al. [18] also investigated the use of gamification for privacy requirements elicitation and engagement with the users. Perera et al. [22] proposed a guide based on the Privacy by-Design framework including a set of best practices to help software engineers to ensure user data privacy during the development of Internet of Things (IoT) applications. Rabinia et al. [24] highlight the difficulty to model the GDPR. This process tends to output models that are extremely complex and hard to understand due to the number of articles of which they are composed, as well as the complexity of both the articles that they contain and the issues that they address. They propose the use of the Formal Legal GRL framework, associated with a methodology to help address the complexity of the models and automate the modelling process. They focus exclusively on design, that is, they do not account for other development phases. BlancoLainé et al. [6] underscore the importance of the GDPR for businesses, which have difficulty understanding the legal requirements. They should take utmost care to ensure compliance, as any mistake can have an impact at all business levels. They attempt to facilitate this process by using enterprise architecture models to represent the GDPR regulation. In addition, there are GDPR-related papers [15] that primarily focus on the process of validating compliance with regulations once the system or application is in use, developing models to automate this process to enable any business, organization or even person to check that its systems or applications comply with the regulations and avoid possible penalties [4][26]. Torre et al. [26] propose analysing articles iteratively in search of keywords to help identify different artefacts and their relationships in order to model GDPR in a machine-readable format [25]. Other approaches, like Ayala-Rivera and Pasquale's GuideMe [4], set out a systematic stepwise approach. They set out six stages in which to analyse the status

of an organization or application, and plan and implement corrective actions to fix non-compliant issues. This is a corrective method for application on existing applications. It is not, therefore, suitable for use throughout the entire software development process but is rather confined to the maintenance activity during which most corrections are usually made. Besides the more functional approaches outlined above, there are a series of best practice guides on compliance developed by different companies and organizations [1]. The EU [14] and companies like Deloitte [11], Norton Rose Fulbright [20] have their own checklists and benchmarks that they make available to their customers with a view to establishing a series of general guidelines enabling a company, organization or even a self-employed worker to assure that their services, applications and infrastructures comply with the regulations.

V. Conclusions and Further Work

We propose a common reference framework to drive the integration of privacy guidelines into the software development process and guarantee personal data privacy. In particular, we provide a reference framework for adopting the articles of the GDPR in the software process and integrate the legal requirements into all the Unified Process activities. Specifically, we adapted each and every one of the 97 articles of the Spanish Law on the Protection of Personal Data and Guarantee of Digital Rights to the Unified Process. This reference framework constitutes comprehensive guidance designed to familiarize a development team with the legal requirements of the regulations throughout all the software development activities, from requirements elicitation to deployment to customers and maintenance. It also provides software development teams with a mechanism for integrating the legal requirements into all the development activity groups of the Unified Process. The development team should include a legal expert in order to take into account all the legal slants and details of specified articles that may be omitted during the use of the reference framework in particular software development projects. One example would be special types of scientific research, historical or medical data processing, which may be especially important in some software projects. A corpus of legal terms shall be developed with experts in natural language processing and legal corpus. Our future research sets out to automate the reference framework advocating the integration of the above professional profiles into software development teams in order to apply natural language processing techniques and automate the reference framework.

Acknowledgment

Work funded by the Spanish Ministry of Science (RTI2018-095255-B-I00) and the R&D programme of Madrid (P2018/TCS-4314).

References

[1] Agencia Española de Protección de Datos (AEDP). Guide of Personal Data Protection for Processing Controllers (In Spanish, Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento), September 2019. https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf

[2] Agencia Española de Protección de Datos (AEDP). Regulatory Compliance List (In Spanish, Lista de cumplimiento normativo), November 2019. [Online]. https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf

[3] J. A. Amorim, R. Ahlfeldt, P. M. Gustavsson, and S. F. Andler. Privacy and security in cyberspace: Training perspectives on the personal data ecosystem. In Proc. European Intelligence and Security Informatics Conf. (EISIC'13), pages 139–142. IEEE, 2013.

[4] V. Ayala-Rivera and L. Pasquale. The grace period has ended: An approach to operationalize GDPR requirements. In Proc. of the IEEE 26th Int. Requirements Engineering Conf. (RE'18), pages 136–146, 2018.

[5] P. Barbosa, A. Brito, and H. O. Almeida. Privacy by evidence: A methodology to develop privacy-friendly software applications. Inf. Sci., 527:294–310, 2020.

[6] G. Blanco-Lainé, J. Sottet, and S. Dupuy-Chessa. Using an enterprise architecture model for GDPR compliance principles. In Proc. of 12th IFIP Working Conf. of The Practice of Enterprise Modeling, (PoEM'19), vol. 369 of Lecture Notes in Business Information Processing, pages 199–214. Springer, 2019.

[7] Boletín Oficial del Estado (BOE). Organic Law 3/2018 on Personal Data Protection and Digital Rights Guarantees (In Spanish, Ley Orgánica 3/2018, de Protección de Datos Personales y Garantías de los Derechos Digitales), December 2018. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

[8] M. Brambilla, J. Cabot, and M. Wimmer. Model-Driven Software Engineering in Practice, Second Edition. Synthesis Lectures on Software Engineering. Morgan & Claypool Publishers, 2017.

[9] A. Cavoukian. Understanding how to implement privacy by design, one step at a time. IEEE Consumer Electron. Mag., 9(2):78–82, 2020.

[10] DAMA International. The DAMA Guide to the Data Management Body of Knowledge DAMA-DMBOK. Technics Publications, 2009.

[11] Deloitte. Deloitte GDPR Benchmarking Survey: The time is now, 2017. https://www2.deloitte.com/lu/en/pages/risk/articles/deloitte-gdpr-benchmarking-survey-the-time-is-now.html

[12] E. Dias Canedo, A. Toffano Seide Calazans, E. Toffano Seidel Masson, P. H. Teixeira Costa, and F. Lima. Perceptions of ICT practitioners regarding software privacy. Entropy, 22(4):429–452, 2020.

[13] European Parliament. Regulation (EU) 2016/679 (General Data Protection Regulation), May 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[14] European Union. GDPR checklist for data controllers, 2018.

[15] European Union. How the GDPR could change in 2020, January 2019.

[16] M. Fowler. Domain Specific Languages. Addison-Wesley, 2010.

[17] I. Jacobson, G. Booch, and J. Rumbaugh. The Unified Software Development Process. Addison-Wesley, 1999.

[18] A. Mavroeidi, A. Kitsiou, and C. Kalloniatis. The role of gamification in privacy protection and user engagement. 2020.

[19] R. Meis and M. Heisel. Computer-aided identification and validation of privacy requirements. Inf., 7(2):28–60, 2016.

[20] Norton Rose Fulbright. GDPR Checklist, 2018. https://www.nortonrosefulbright.com/en/knowledge/publications/3b14a527/gdpr-checklist

[21] UML 2.5.1 Specification. https://www.omg.org/spec/UML/

[22] C. Perera, M. Barhamgi, A. K. Bandara, M. A. Azad, B. A. Price, and B. Nuseibeh. Designing privacy-aware internet of things applications. Inf. Sci., 512:238–257, 2020.

[23] PricewaterhouseCoopers US. GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, January 2017. https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html

[24] A. Rabinia, S. Ghanavati, L. Humphreys, and T. Hahmann. A methodology for implementing the formal Legal-GRL framework: A research preview. In Proc. of 26th Inter. Conf. Requirements Engineering: Foundation for Software Quality, (REFSQ'20), LNCS vol. 12045, pages 124–131. Springer, 2020.

[25] D. Soltes. Social networks as the best instrument for achieving full, worldwide and truly global e-inclusion. Proc. 16th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI'), pages 142–146, 2012.

[26] D. Torre, G. Soltana, M. Sabetzadeh, L. C. Briand, Y. Auffinger, and P. Goes. Using models to enable compliance checking against the GDPR: An experience report. In Proc. of the ACM/IEEE 22nd Int. Conf. on Model Driven Engineering Languages and Systems (MODELS'19).