Agile Teams' Perception in Privacy Requirements Elicitation: LGPD's compliance in Brazil

1st Edna Dias Canedo
Department of Computer Science
University of Brasília (UnB)
Brasília–DF, Brazil
ednacanedo@unb.br

2nd Angelica Toffano Seidel Calazans
University center – UniCEUB
Brasília–DF, Brazil
angelica.toffano@gmail.com

3rd Anderson Jefferson Cerqueira
Department of Computer Science
University of Brasília (UnB)
Brasília–DF, Brazil
andersonjcdf@gmail.com

4th Pedro Henrique Teixeira Costa
Department of Computer Science
University of Brasília (UnB)
Brasília–DF, Brazil
phtcosta@gmail.com

5th Eloisa Toffano Seidel Masson
University center – UniCEUB
Brasília–DF, Brazil
eloisa.masson@ceub.edu.br

2021 IEEE 29th International Requirements Engineering Conference (RE) | 978-1-6654-2856-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/RE51729.2021.00013

***Abstract*—Context: The implementation of the Brazilian General Data Protection Law (LGPD) may impact activities carried out by the software development teams. It is necessary for developers to know the existing techniques and tools to carry out privacy requirements elicitation. Objectives: In this research, we investigated the perception of agile software development team members from different organizations, regarding the impact that LGPD will have on the activities of the software development process. Methods: We conducted an online survey and a systematic literature review to identify the techniques, methodologies and tools used in the literature to perform privacy requirements elicitation in the context of Agile Software Development (ASD). In addition, we also investigated the perception of an agile team from a Federal Public Administration organization regarding the impacts of the obligation to develop software in accordance with the LGPD. Results: Our findings reveal that agile teams know the concepts related to data privacy legislation, but they do not use the techniques proposed in the literature to perform privacy requirements elicitation. In addition, agile teams face problems with outdated software requirements specifications and stakeholders' lack of knowledge regarding data privacy. Conclusions: Agile teams need to improve their knowledge on privacy requirements.**

***Index Terms*—Privacy Requirements Elicitation, Agile Teams, Perception, LGPD**

I. Introduction

Data privacy has become a major concern in software development, mainly due to the requirements of data protection laws, such as the General Data Protection Regulation (EU) 2016/679 (GDPR) [1] and the Brazilian General Data Protection Law (LGPD) [2]. Data privacy violations can be prevented if privacy requirements are set correctly during the early stages of the software development process [3]. According to Thomas and Blaine [4], privacy can be considered as a non-functional requirements, because its focus is on obtaining and processing large amounts of users' personal data.

Several research studies have identified that software developers lack knowledge of software privacy and that they do not have the technical knowledge necessary to develop systems that work with sensitive data [5]. In addition, software developers do not know the principles of data privacy and when building software, they make ad hoc decisions and do not worry about the best practices developed by the academy to facilitate requirements elicitation and ensure data privacy of users. This behavior probably occurs due to the lack of knowledge of the existing techniques and methodologies [6].

In requirements elicitation, agile teams work with stakeholders to understand the application domain, operational constraints, functional and non-functional requirements [7]. Agile methodologies recognize that requirements change constantly, evolve over time and that they are discovered throughout the software development process [8]. Agile software development has several benefits, such as improved user satisfaction, changing requirements definition during any phase of the development process, frequent software delivery, and close stakeholder interaction [9]. According to Wagner et al. [10] non-functional requirements elicitation in agile software development is still neglected during its definition and documentation.

This paper investigates the perception of agile teams regarding the impact that LGPD will have on their activities during software development, as from August 2020 all software development processes in Brazil should be LGPD compliant [2]. Thus, we investigated whether agile teams correctly interpret privacy principles and implement these concepts and principles during software development, as well as what actions can be taken to reduce the impact of the need to implement systems, according to data privacy laws by agile development teams, and to achieve this goal, we conducted a systematic literature review. Based on the findings of the review, a survey and focus group were conducted aiming to investigate and characterize agile team perception. Data collected from studies, observations and interviews with software developers were analyzed and synthesized [11].

The main contribution of our work is the understanding of the perception of agile teams regarding difficulties they

978-1-6654-2856-9/21/$31.00 ©2021 IEEE
DOI 10.1109/RE51729.2021.00013

face in implementing privacy requirements and how LGPD compliance will impact their daily activities. Results show that those who are responsible for documenting requirements elicitation artifacts are demanded to maintain them up to date, detailing all privacy requirements correctly, avoiding rework for developers. In addition, up-to-date documentation allows users to hold a better understanding when consenting to the disclosure of their personal data, as well as facilitating the implementation of functionalities by developers.

II. Background and Related Works

A. Agile Methodologies and Requirements Engineering (RE)

Agile Software Development (ASD) is increasingly being used by software industry, as reported by [12], [13]. ASD is characterized by a focus on customer needs, the business value of deliveries, stakeholder engagement, short iterations and fast deliveries. People and interactions are at the center of these methodologies [14]. Agile methodologies such as Scrum, Extreme Programming (XP), Dynamic Systems Development Method (DSDM) and Lean provide a process for developing software products in accordance with the principles and values defined by the Agile Manifesto [15], [14], [16]. Considering the context of software development, there is a consensus between the literature and industry that requirements are the basis for all software products. Thus, Requirements Engineering (RE) plays an important role in the development of a software. The traditional RE approach defines, according to Sommerville [17], the following activities: feasibility study, elicitation and analysis, specification and validation.

Regarding agile methodologies, the RE approach is distinct from the traditional RE approach; the phases are clearly separated and they are mixed and repeated at each iteration, in consonance with Kassab [18]. Darrin and Devereux [14] assert that the emphasis on customer proximity in collaboration with the system developer – in defining and changing requirements – enables a more comprehensive understanding of the user's environment and needs, improving the quality and applicability of the system requirements.

Heikkila et al. [19] report the following advantages of the agile RE approach: lower process overheads, improved requirements understanding, reduced overburden, responsiveness to change, fast delivery and validation, and improved customer relationships. The authors also identified some challenges of this approach, such as issues with client or customer representatives, insufficiency of the user story format, difficulties in the prioritization of requirements, non-functional requirements elicitation [10], among others. Schon et al. [20] identified User Story, Prototype and Use case as the most commonly used techniques for requirements elicitation in the context of agile methodologies. In the work presented by Kassab [18], the use of the user story technique in requirements elicitation in agile software development is also reported.

ASD does not provide an approach to guide the elicitation and specification of privacy requirements using a specific technique. According to Gurses and Álamo [21], empirical studies are still needed to explore how privacy issues are (or are not) currently addressed in different engineering contexts. In their view, it is crucial to assess which methods, techniques, and tools are most appropriate in a given software privacy context complying with current laws and regulations.

B. Brazilian General Data Protection Law (LGPD)

In August 2020, Law No. 13,709 - Brazilian General Data Protection Law (LGPD) [2], which provides for the protection of personal data, came into force. The aforementioned Law applies to organizations in Brazil and also organizations that are not physically located in Brazil, but offer goods and services or process personal data in Brazil. The main purpose of the Act is the processing of personal data of individuals, that is information related to an identified natural person, such as name, age, marital status, documents, etc., performed by controllers and processors [2]. Regarding to the context of data privacy, several models were proposed with principles similar to LGPD [22], [23], among them ISO/IEC 29100 - Information technology — Security techniques — Privacy framework [24] and the General Data Protection Regulation – GDPR [1], [25]. GDPR started effect in the European Union (EU) on May 25, 2018, through the Regulation EU 2016/679 [1].

According to Data Guidance by OneTrust [26], LGPD and GPDR have many similarities with a few disagreements regarding the processing of individuals' personal data. LGPD provides ten principles while GDPR provides seven [27]. It must be highlighted that ISO/IEC 29100 [24] has twelve principles and most part of these principles are similar to GDPR [1], [25] and LGPD principles [2], other principles are referred as "individual rights" or "legal bases". For example, Consent and Choice is a principle in ISO/IEC 29100 [24], however, it is considered a legal basis/individual right in LGPD and GDPR.

Ayala-Rivera and Pasquale [25] and Otto and Anton [28] mention that regulations are usually vaguely formulated, may contain ambiguities, crossed references and domain specific definitions, making it difficult for IT professionals to extract and operationalize privacy requirements. Regardless of the model adopted by the country or organization, several authors identify the need to study the views of information and communication technology (ICT) practitioners on privacy and the organization's position on privacy, among other aspects [5], [29].

C. Privacy versus Agile Methodologies

Privacy is the ability of an individual to control their own information [30]. Privacy violations can be prevented if privacy requirements are properly identified/elicited during the initial stages of software development at the requirements specification stage. Thus, privacy becomes increasingly important in the way users rely on software to perform their daily activities [30]. The increased interest in the subject of privacy and requirements in recent years has been recognized by several authors [21], [31]. Privacy Engineering, according to Gurses and Álamo [21], encompasses the following aspects:

privacy engineering methods, privacy engineering techniques and privacy engineering tools.

Regarding the concepts of privacy, requirements elicitation and agile methodologies, a considerable amount of work covering the aspect of privacy engineering methods and requirements [32], [33], [34] can be found in the literature. However, there is a small amount of work focused on privacy techniques – which relate to procedures, prescribed language or notation, for performing privacy engineering tasks or activities – and requirements, especially when these techniques are related to agile methodologies and specifically to user story and use case. Using user story and use case techniques, Bartolini et al. [35], in order to be compliant with GDPR principles, suggest the creation of Access Control Policies (ACPs) aligned with the principles of GDPR and the user stories. The work presented by Rygge et al. [36] suggests the use of Threat Poker to help identify security and/or privacy risks during agile software development.

III. Study Settings

To investigate the problem, we conducted a systematic literature review (SLR), according to the guidelines proposed by Kitchenham et al. [37]. The SLR was composed of automatic and manual searches, performed in digital libraries. The SLR was performed to identify the methodologies and techniques used for privacy requirements elicitation during the agile software development process. We have identified several methodologies and techniques used in the literature. In this work, in order to verify if the identified methodologies and techniques are used in the industry by the agile software development teams, we conducted an online survey with several developers of agile teams. In addition, we also held a focus group with agile team developers from a Federal Public Administration (FPA) organization, responsible for information security for the federal government, to find out if they used these techniques during privacy requirements elicitation and/or knew about these methodologies and techniques.

We used triangulation to perform data analysis. The data triangulation aims to cover the breadth in the description, explanation and understanding of the study under analysis [38]. Data triangulation uses different data sources, including different times for data collection, different locations for data collection, and different people who may be involved in the study. The starting point is to explicitly and systematically involve people and study groups, local and temporal configurations in the study [39]. We performed data analysis through triangulation using 3 sources: (1) systematic literature review, (2) survey and (3) focus group. Figure 1 presents the details of data triangulation adopted in this research.

A. Systematic Literature Review

The steps for conducting a systematic literature review (SLR) involve the planning, execution and analysis of results. The planning phase consists of designing all the details necessary for the review to be carried out [37]:

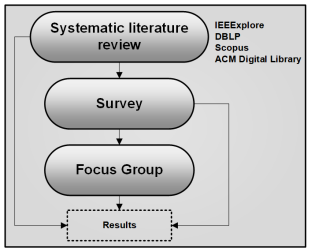


Fig. 1. Adopted Data Triangulation Scheme

1) Definition of the review protocol: it consists of specifying the research questions to be answered and the method to be followed to answer them;
2) Definition of the search strategy: it consists of specifying the automatic search process of the studies. As a complementary mechanism, manual search strategies can be defined;
3) Definition of inclusion and exclusion criteria: it consists of establishing criteria that specify the decision process on which publications found by the search strategy will be included in the review;
4) Definition of quality criteria: classification of selected publications according to a taxonomy to assess the level of the study in terms of consistency of the research objectives, clarity of the context description, suitability of the selected method to the type of study, etc.;
5) Definition of the results interpretation process: it consists of defining how the relevant data will be extracted, analyzed, stored and reported.

The execution phase involves the search, selection and evaluation of studies (called primary studies) in accordance with the inclusion and exclusion criteria defined in the protocol. Once the studies have been selected, data from the included primary studies can be extracted and synthesized during the results analysis phase.

1) Research Questions: We have defined the following research questions to conduct the systematic literature review:

RQ.1 How do agile teams implement the concept of privacy in their daily work? (namely, current privacy practices adopted)
RQ.2 How do agile teams interpret the concept of privacy regarding to the Brazilian General Law of Personal Data Protection implemented in 2020? (namely, what are the future privacy practices)
RQ.3 How do agile teams perceive actions that should be adopted to reduce the impact of privacy in agile software development?

2) Search Strategy: We proposed a protocol to specify the steps and criteria involved in carrying out the SLR. A review protocol includes details of how different types of studies are to be found, evaluated and synthesized [40]. In the protocol were defined the research questions, the search strategies adopted to identify the relevant primary studies, the search string to use in the databases, the exclusion/inclusion

criteria and the quality assessment criteria. In addition, the data extraction and analysis process were determined. The strategy for collecting the studies contained the following steps: (i) automatic search of electronic databases, (ii) manual search of journals, conferences and workshops, (iii) analysis of the reference lists of other secondary studies in privacy requirements elicitation, known as snowballing.

We used the following digital bases for automatic search: ACM Digital Library, IEEE Xplore Digital Library, Scopus and dblp computer science bibliography. The search strings adopted were: TITLE-ABS-KEY ("requirements engineering" OR "requirements approach" OR "requirements methodology" OR "requirements process" AND ("elicitation" OR "requirements elicitation" OR "requirements specification" OR "requirements gathering" OR "requirements capture") AND ("technique" OR "method" OR "tool") AND ("agile software development" OR "agile development")) AND ("privacy" or "security")).

3) Selection Criteria (Inclusion and Exclusion): We have defined the following selection criteria for the selection of primary studies: 1. The work must be available in the digital databases previously defined. 2. The year of publication of the studies must be between 2005 and 2020. However classic sources with definitions (books with classic concepts or pioneering articles) can also be considered. 3. The work must be related to the context of privacy requirements elicitation. 4. The study should propose or use/evaluate existing methods, methodologies, techniques or tools to perform privacy requirements elicitation in the context of agile software development.

As a criteria for exclusion from studies, we consider the non-fulfillment of any of the inclusion criteria, as well as: 1. Works published as short paper; 2. Do not presenting enough information to extract the expected data, thus impairing the quality or relevance of the work.

4) Quality Criteria: The evaluation of the quality of the studies identified by the search strategy execution made it possible to select the most relevant articles to compose the SLR that was executed using the four selection steps of studies [40]; 1. Search strategy execution involving automatic and manual searches. After that, a preliminary list of studies was generated, and with the help of StArt tool it was possible to discard duplicate jobs immediately; 2. Identification of potentially relevant studies, based on reading the title and abstract. In this step, it was possible to discard studies that were clearly irrelevant to the research. In case of doubt about the permanence of any study in SLR, the next step helped to decide; 3. Reading of the introduction, methodology and conclusion of the pre-selected works, applying again the inclusion and exclusion criteria; 4. The works selected in step 3 were read in full and the volume of studies resulting in this step (23 primary studies) were used to compose the SLR and support the answers to the research questions.

5) Systematic Literature Review Results: The automatic search on digital databases resulted in a total of 34 studies and the manual search performed in the Annals of Conferences and Journals resulted in a total of 9 studies (43 pre-selected articles). After applying all the steps of the paper selection strategy, a total of 23 primary studies to be used in data extraction were identified. Table I shows the primary studies used in the SLR.

B. Survey Analysis

We designed a survey aimed at understanding the perception of developers participating in projects using agile methodologies. Participants had to indicate their agreement or disagreement with statements derived from the analysis questions, which represented assertions that not all of our survey participants agreed on. Answer options ranged from strongly disagree to strongly agree, at 5 points Likert scale with a neutral option. The survey contained 30 questions. The estimated time to answer our survey was ten minutes. We selected participants from software development companies. In total, 82 people accessed the survey online, but only 70 participants completed the survey. The survey was performed with people from distinct organizations and places.

C. Focus Group

To complement the answers of the survey and the research questions defined in Section III-A1, we conducted a focus group with developers from a public agency responsible for the Brazilian federal government's security, to understand their perceptions regarding LGPD compliance. Focus groups are carefully planned discussions, designed to obtain the perceptions of the group members on a defined area of interest. There are typically between three to twelve participants and the discussion is guided and facilitated by a moderator, who follows a predefined structure so that the discussion stays focused. The members are selected based on their individual characteristics as related to the session topic [61].

The focus group was performed in three phases. In the initial phase (*defining the research problem*), we established the focus group objective as our interest in verifying that the agency's developers were working with LGPD guidelines, as well as what impacts this law could have on their activities – due to the need for their systems to be LGPD compliant. In the second phase (*participant selection*), the profile of the participants was defined: members of the team responsible for developing systems functionalities according to privacy requirements specifications. Interviews were conducted with the participants to identify theoretical and practical knowledge in the context of requirements, privacy and agile models. Eleven participants from this team were selected, having the necessary knowledge to develop software according to specification documents. The group of participant is composed of key developers and the project manager of the agile software development team.

In the third phase (*executing the focus group session*), gathering of information was performed using the focus group technique. We held eight meetings with the participants; each meeting lasted two hours and was carried out at the agency's premises. The focus group was led and managed by a member of the agency's project team, responsible for the systems

ID	Title	Reference
S1	Privacy Requirements Engineering in Agile Software Development: a Specification Method	[41]
S2	PCM tool: privacy requirements specification in agile software development	[32]
S3	Requirements engineering: A systematic mapping study in agile software development	[42]
S4	A Requirements Engineering Techniques Review in Agile Software Development Methods	[43]
S5	Privacy by Design in Agile Software Development	[44]
S6	Security and Privacy as Hygiene Factors of Developer Behavior in Small and Agile Teams	[45]
S7	Metrics to Meet Security - Privacy Requirements with Agile Software Development Methods in a Regulated Environment	[46]
S8	Empathy and Criativity in Privacy Requirements Elicitation: Systematic Literature Review	[47]
S9	Experiences in the Development and Usage of a Privacy Requirements Framework	[48]
S10	Security, Compliance, and Agile Deployment of Personal Identifiable Information Solutions on a Public Cloud	[49]
S11	The Odyssey: modeling privacy threats in a brave new world	[50]
S12	Aligning Security Objectives With Agile Software Development	[51]
S13	An Empirical Perspective on Security Challenges in Large-Scale Agile Software Development	[52]
S14	Towards a Secure SCRUM Process for Agile Web Application Development	[53]
S15	GDPR-Based User Stories in the Access Control Perspective	[35]
S16	Identifying How the Brazilian Software Industry Specifies Legal Requirements	[54]
S17	Perceptions of ICT Practitioners Regarding Software Privacy	[27]
S18	Information Security in Agile Software Development Projects: a Critical Success factor Perspective	[55]
S19	The Security Intention Meeting Series as a way to increase visibility of software security decisions in agile development projects	[56]
S20	Towards Risk-Driven Security Requirements Management in Agile Software Development	[57]
S21	Collaborative security risk estimation in agile software development	[58]
S22	Threat modelling and agile software development: Identified practice in four Norwegian organisations	[59]
S23	Using the Design Thinking Empathy Phase as a Facilitator in Privacy Requirements Elicitation	[60]

TABLE I
SELECTED PRIMARY STUDIES IN SYSTEMATIC LITERATURE REVIEW

documentation and co-author of this research. Initially, the moderator explained, to the participants, the objectives of the focus group and the expectations of its execution. Furthermore, questions were targeted to participants by the moderator. The moderator's role was to lead the activity and have the participants describe how their daily activities were being performed and their compliance with LGPD [2].

IV. RESULTS

A. SLR Results

Most selected primary studies propose a technique, method or tool to address privacy or security in the context of agile software development [41], [32], [46], [48], [49], [53], [35], [56], [57], [58]. Other selected works were Requirements Engineering reviews; although they do not deal specifically with privacy, these studies show some results related to data privacy [43], [42]. Other works identified challenges and opportunities in the context of agile teams, privacy and privacy by design and security [50], [44], [51], [52], [54], [55], [59], [60], [47]. Some studies have analyzed the behavior and perceptions of ICT practitioners in relation to privacy [45], [27].

B. Survey Results

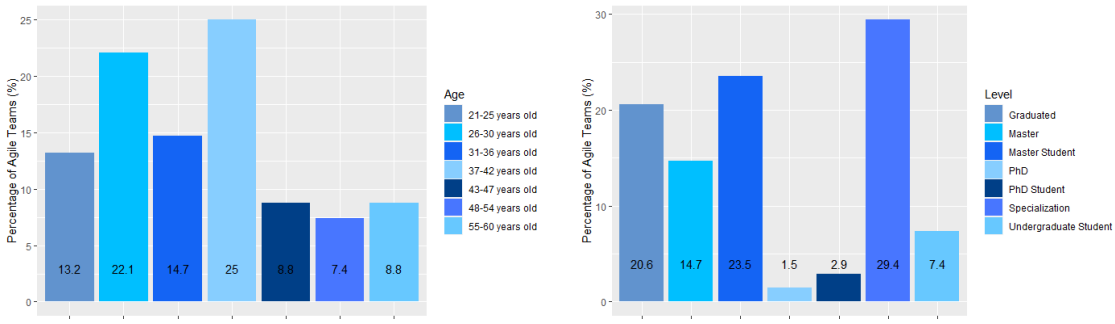
13.2% of survey participants are between 21 and 25 years old, 22.1% are between 26 and 30 years old, 14.7% are between 31 and 36 years old, 25% are between 37 and 42 years old, 8.8% are between 43 and 47 years old, 7.4% are between 48 and 54 years old and 8.8% are between 55 and 60 years old, as shown in Figure 2 (a). 7.4% of survey participants are undergraduate student, 20.6% are graduated, 29.4% have specialization degree, 23.5% are master student, 14.7% are masters, 2.9% are PhD student and 1.5% are PhD, as shown in Figure 2 (b).

5.9% of survey participants have up to one year of experience, 8.8% have between 11 and 15 years, 10.3% have between 1 and 3 years, 14.7% have between 4 and 6 years, 19.1% have between 16 and 20 years, 20.6% have between 7 and 10 years and 20.6% have more than 21 years of experience, as shown in Figure 3 (a). 33.1% of survey respondents work/worked in private software development companies, 27.1% work/worked in Federal Public Administration agencies, 18.8% work/worked in research/collaboration projects, 15.8% work/worked in state-owned company and 5.3% work/worked in open source software projects, as shown in Figure 3 (b).

As all survey respondents work in agile teams, we chose to use, in this research, the term "agile teams" to categorize the participants. Most of the agile teams interviewed work at private software development companies or Federal Public Administration Agencies. Regarding the methodologies – that agile teams have used or are currently using, 61.9% of respondents said they were working or have worked with the Scrum agile methodology, 26.2% work with XP, 8.3% work with Lean and 3.6% work with Kanban. With this result it is possible to conclude that all agile teams know and work with the Scrum agile methodology.

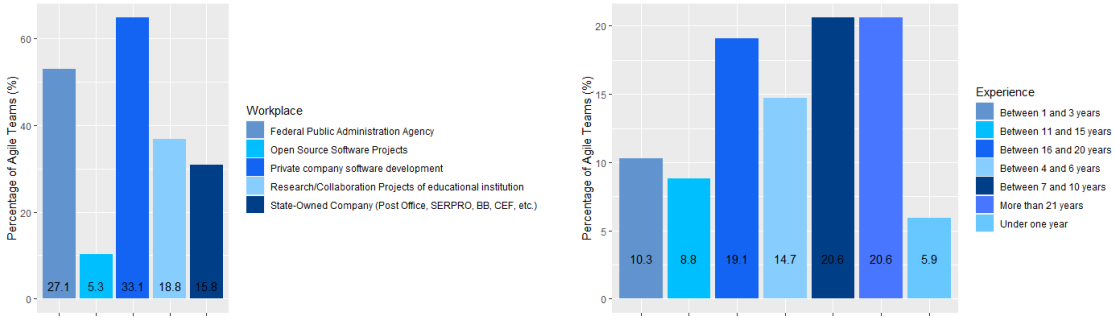
The 14th Annual State of Agile Report [13], identified that 24% of survey respondents work with Scrum (Scrum of Scrums, Large Scale Scrum (LeSS), Enterprise Scrum). Meier and Kropp [12] identified that 59% of software development companies located in Switzerland said they use Scrum, 9% said they used Lean/kanban and 3% said they use XP.

The work presented by Alsaadi et al. [62] investigated the use of agile methodologies in the requirements elicitation of the European Medical Device Regulation (MDR), as requirements needed to be in compliance with the legisla-



(a) (b)

Fig. 2. Figure (a) shows the age of the Agile Teams , while (b) shows the level of the Agile Teams.



(a) (b)

Fig. 3. Figure (a) shows the workplace of the Agile Teams, while (b) shows the experience of the Agile Teams.

tion. The authors concluded that XP was unsuitable for the MDR requirements elicitation as it had no fixed planning and documentation was insufficient to address privacy. Scrum was considered adequate to do the requirements traceability, although it also had insufficient documentation to proper document the requirements. Feature-Driven Development (FDD) was considered the most suitable agile methodology for MDR requirements elicitation. In the context of this research, there was no participation of developers who had knowledge about FDD.

Rygge and Jøsang [36] proposed Threat Poker as a team-based method to be exercised during agile software development for assessing both security and privacy risk, and for evaluating the effort needed to remove corresponding vulnerabilities in the developed software. The authors used Scrum agile methodology and User Stories for system requirements elicitation in an attempt to test the Threat Poker method.

Summary: The results found allow us to infer that a significant portion of agile teams know Scrum methodologies. Our research reinforces the findings of Meier and Kropp [12] and Agile report [13].

1) RQ.1. How do agile teams implement the concept of privacy in their daily work? (namely, current privacy practices adopted): In an attempt to answer RQ.1 we elaborated questions focused on the understanding of software privacy concepts by agile teams, as well as which practices are adopted in agile projects that they engage. Table II presents the results obtained with respect to the Privacy Principles, Known Principles and Used Principles. Regarding the privacy solutions adopted, the most distinguished ones were User's control (79,2%), User's Access (71,5%), Encryption (58,5%) and Automatic Expiration data (30,8%). The least mentioned were the solutions related to Decentralization (7.7%) and Turn off data Collection (4,9%).

Privacy Principles	**% Known Principle**	**% Used Principle**
Consent and choice	53.8%	30.8%
Transparency	52.5%	20.5%
Security	46.2%	100%
Needs	38.5%	15.4%
Purpose	30.8%	61.5%
Open Access	28.7%	10.2%
Prevention	25.3%	69.2%
Accountability and Legal Reporting	24.5%	46.2%
Non-discrimination	23.1%	21.3%
Adequacy	15.4%	23.1%
Data Quality	15.2%	28.8%

TABLE II
PRIVACY PRINCIPLES KNOWN TO AGILE TEAMS

Summary: From the results presented in Table II it can be concluded that the privacy principles most known to agile teams are: consent and choice, transparency and security. Principles that are most commonly used in projects are: Security, Prevention and Purpose. In addition, the most adopted solutions are: User's Control, User's Access and Encryption.

2) RQ.2. How do agile teams interpret the concept of privacy in Brazilian General Law of Personal Data Protection implemented in 2020? (namely, what are the future privacy practices): Agile teams have stated to know about LGPD, 45% considering they have the knowledge to implement the principles regulated by the law in their agile software development activities. Moreover, 84% of agile teams declared that organizational environment interferes with privacy practices and 54.8% reported that organizations in which they work have informed them about the importance of systems, that are developed or used by the organization, to be LGPD compliant from 2020 onwards. This result differs from with research by Bednar et al. [29] which identified developers' difficulty in understanding and following new privacy-related regulations. The result obtained also differs from the results of Canedo et al. [27], which identified that ICT practitioners lack a comprehensive knowledge of software privacy. It is possible to infer that the result obtained in this research is due to the fact that the organization in which the focus group participants work has a greater concern with information security and data privacy.

Agile teams are favorable that organizations disclose organizational privacy procedures to all company professionals, and that organizations create organizational policies focused on the privacy and data security solutions adopted to engage the organization's professionals in ensuring and respecting these principles. This result confirms the result of the research carried out by Canedo et al. [27].

Summary: Agile teams know about LGPD and agree that the organizational environment interferes with privacy practices and that organizations should propose and disclose organizational policies aimed at privacy and security.

3) RQ.3. How do agile teams perceive actions that should be adopted to reduce the impact of privacy in agile software development?: Regarding agile teams' perceptions that are related to actions that should be taken to reduce the impact of privacy in agile software development, some suggestions were selected from the literature. The respondents had to declare their agreement or disagreement with each item. The following obtained results were:

- The criteria used to determine which work items are critical to privacy should be based on data protection objectives, 22.3% of agile teams strongly agree, 71.7% agree and only 6% of respondents were neutral, as presented in Q1 in Figure 4.
- Participants did not have a consensus about the question "in eliciting requirements, deciding in advance on a fixed set of privacy requirements could compromise the speed of the development process". The results obtained for this question were: 6.3% of agile teams strongly agree and 37.7% agree, 12% strongly disagree and 26% disagree. 17% of agile teams were neutral, as shown in Q2 in Figure 4.
- Regardless of the data protection set selected as the initial base, they should be able to evolve over future project iterations, 37.7% of agile teams strongly agree and 60.3% agree and 2% were neutral as shown in Q3 in Figure 4.

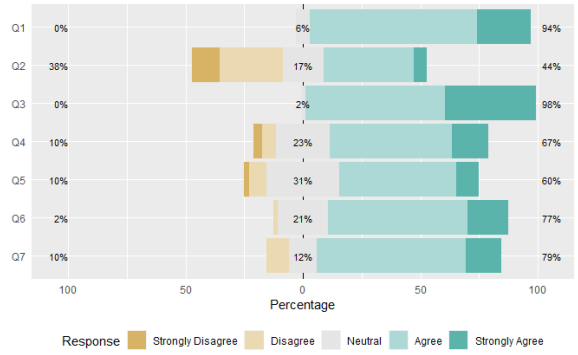


Fig. 4. Agile Team's Perception

- Concerning the use of documents that are not currently required when using agile methodology, such as: data flow diagram, architecture overview, data model overview and/or class diagram to identify information flow related to privacy and where the personal data used in the system reside could facilitate and document the privacy requirements, 16% of agile teams strongly agree and 51% agree, 3% strongly disagree and 7% disagree. 23% of agile teams were neutral in relation to the use of these documents as facilitators, as shown in Q4 in Figure 4.
- Data model or class diagram can be used as part of the iterative workflow to retain accurate privacy information with minimal documentation effort, 10.4% of agile teams strongly agree and 49.6% agree, 2.7% strongly disagree and 7.3% disagree. It is worth highlighting that, 31% of agile teams were neutral about this statement, as shown in Q5 of Figure 4. These findings partially ratify authors as Alsaadi et al. [62] who consider the use of UML modeling (from FDD agile methodology) more suitable for privacy requirements elicitation for the reason that it has a more extensive documentation.
- To minimize the added overhead associated with the privacy impact of each work item, the process can be divided into several phases. The first phase would occur during the sprint planning. For each work item accepted in the sprint, a decision should be made whether this work item includes aspects related to privacy sensitive areas or not. In this question, 17.5% of agile teams strongly agree and 59.5% agree with this statement and only 2% of agile

teams disagree and 21% were neutral, as shown in Q6 in Figure 4.

- Each privacy policy specification can refer to a system usage scenarium, such as a user story or use case that begins with the specification of the basic information. 14.8% of agile teams strongly agree and 64.2% agree and only 10% of agile teams disagree and 12% were Neutral, as shown in Q7 in Figure 4. This answer confirms the work of Bartolini et al. [35] that use Data Protection backlogs, which are lists of user stories about GDPR provisions told as technical requirements. For each user story they build a corresponding Access Control Policy, enabling the implementation of GDPR compliant Access Control systems. Peixoto et al. [32] developed the Privacy Criteria Method (PCM) Tool, which is an approach designed to guide the specification of privacy requirements in agile software development. Privacy requirements can be specified in this tool using a user story or a use case.

In the survey we investigated three discursive questions to learn about teams' perceptions of some aspects of software privacy. The first question was related to the use of user stories by agile teams, in order to identify when and how privacy aspects are inserted in user stories, such as consent, documentation and accountability. For this discursive question twelve answers were obtained and seven of them (58%) identified that the moment would be during the creation and/or prioritization of user stories. Some answers obtained are: "In the user story as an additional feature" and "In the acceptance criteria during the creation of user stories." "In the Planning phase" received two answers and "In the definition of business processes", "Throughout the development process" and "On user consent" were mentioned only once by the agile team members.

Among the difficulties reported by the agile teams in working with user stories that are related to the implementation of privacy principles, such as consent, documentation, accountability, and so on, the following results were obtained: i) Difficulty in placing privacy criteria in user stories (3 participants); ii) Lack of knowledge of the law by developers and users (2 participants); iii) Difficulty with documentation and accountability (2 participants); iv) Difficulty with consent, as "not all the users have the awareness and knowledge to define them" (2 participants).

Other difficulties, such as: "Outdated user story", "Requirements definition changes", "Test complexity" and "No difficulties" were each one identified by one participant.

Bartolini et al. [35] investigate the use of User Stories in the access control according to the GDPR. The authors concluded that, although user stories are informal, they must be well described and related to "access control rules" and to what is specified in the GDPR. Thus, in case of modifications in GDPR, user stories can help detect rules that need to be updated. We can infer that the proposal of Bartolini et al. [35] could minimize some of the difficulties mentioned: "Difficulty in placing privacy criteria..." and "Difficulty with documentation ..." and "Requirements definition changes".

Regarding other practices that should be used by agile teams to implement privacy as proposed by LGPD, participants cited the use of Canvas, Design Sprint [63], and Design Thinking [64], using a minimum viable product (MVP) [65] to understand, in a narrow scope, how some privacy requirements are implemented to meet a business need. Moreover, it was mentioned that the implementation of privacy should be performed by the development team, especially regarding technical aspects such as data encryption, anonymization, etc. However, demands related to the LGPD should be handled at an organizational level and should be another type of requirements demanded by the requesting areas during the definition of the software scope.

C. Focus Group Results

Table III presents the summary of the focus group participants. The focus group session result was documented in notes and audio used during the sessions. All participants have experience in agile software development and they use user stories to document software requirements. Participants reported that in their daily activities they are concerned with implementing the concepts of privacy and adopting practices already known and consolidated in the literature to implement the privacy requirements.

ID	Role	Degree	Experience
P1	Project Manager	Master	18 years
P2	Developer	Master Student	15 years
P3	Developer	Graduated	10 years
P4	Developer	Graduated	8 years
P5	Developer	Graduated	6 years
P6	Developer	Master	6 years
P7	Developer	Graduated	6 years
P8	Developer	Graduated	4 years
P9	Developer	Graduated	4 years
P10	Developer	Master	3 years
P11	Developer	Master	2 years

TABLE III
FOCUS GROUP PARTICIPANTS

The focus group participants stated that in their organization the software development process is carried out according to the Scrum Agile Methodology [66]. In the survey, most participants also use the Scrum Agile Methodology. For the focus group, we have defined the questions considering the results of the SLR, the survey and the research objectives. So, we conducted the discussion with the participants by asking the following questions to complement the responses from **RQ.1**. How do agile teams implement the concept of privacy in their daily work? (namely, current privacy practices adopted):

RQ.1:Q1. How do you implement privacy concepts/practices in your daily activities?

RQ.1:Q2. What are the most used privacy principles in your organization?

RQ.1:Q3. What are the most used solutions/practices in your organization?

Regarding RQ.1:Q1, the focus group participants informed that they implement the privacy concepts through the acceptance criteria, which are documented in the user stories. This

finding in the focus group confirms the results found in the survey: 79% of participants also reported that they are using user stories and the results found by Bartolini et al. [35]. The most widely used privacy principles they use are security, prevention and data quality (RQ.1:Q2). This result is partially in line with the survey result, which identified security with 100% and prevention with 69.2% of use.

Regarding RQ.1:Q3, the most widely adopted privacy solutions are encryption, user access and user's control. This result ratifies the results obtained with the survey, which identified Encryption, User's access and User's control with 58%, 71.5% and 79.2%, respectively. Ayalon et al. [67] and Hadar et al. [5] had already identified in their studies that Encryption, User's Control and User's Access solutions as the most widely used and well-known practices, in the perception of the developers. This ratifies part of our outcomes. These results confirm part of the results of Canedo et al. [27] which identified in their research with ICT practitioners (not considering age models) the use of similar principles and solutions.

Summary: Privacy requirements can be specified using a user story. The most widely adopted privacy solutions are encryption, user access and user's control.

To complement the responses from **RQ.2**. How do agile teams interpret the concept of privacy in Brazilian General Law of Personal Data Protection implemented in 2020? (namely, what are the future privacy practices) we asked the following questions:

RQ.2:Q1. Do you have extensive knowledge of the Brazilian General Law of Personal Data Protection (LGPD)?

RQ.2:Q2. What are the impacts and challenges between current privacy practices and the principles defined by the Brazilian General Law of Personal Data Protection (LGPD)?

RQ.2:Q3. Does the organizational environment interfere with privacy practices? Positively or negatively?

Regarding to LGPD knowledge, 100% of participants know the law and are comfortable implementing all established data privacy guidelines (RQ.2:Q1). Furthermore, they stated that LGPD will not have much impact on their software development activities as they already work with most of the requirements suggested by the law (RQ.2:Q2).

This result differs from the result found in the survey, where approximately 45% believed they had the necessary knowledge to implement the principles regulated by the law. One of the possible reasons for this finding can be the fact that the agency in which the focus group participants work has a great concern for information security. All participants in the focus group stated that privacy practices positively interfere with the activities they perform (RQ.2: Q3). This result confirms the findings of the survey, where 84% of agile teams declared that organizational environment interferes with privacy practices.

Summary:The organizational environment interfere with privacy practices.

To complement the responses from **RQ.3**. How do agile teams perceive actions that should be adopted to reduce the impact of privacy in agile software development? We selected results obtained in SLR about privacy and agile models, and we sought to ratify or rectify those results.

RQ.3:Q1. Should the definition of critical work items also consider privacy principles?

RQ.3:Q2. Can deciding in advance on a fixed set of Privacy Requirements compromise the agility of the development process?

RQ.3:Q3. Can Privacy Requirements be documented with the use of documents, such as: data flow diagram, architecture overview and an overview of the data model and class diagram to identify the flow of information related to privacy and where the data resides personal data used in the system?

RQ.3:Q4. Can the data model or class diagram be used to retain accurate privacy information with a minimum of effort spent on documentation?

RQ.3:Q5. Can each specification of privacy criteria refer to a system usage scenario, such as a user story or use case?

RQ.3:Q6. What difficulties do you identify, related to the implementation of privacy principles (consent, documentation, accountability, among others) in the agile development process when using user stories?

RQ.3:Q7. What practices/actions do you think should be used by agile teams to implement data privacy, as proposed by the LGPD, and with minimal impact?

The focus group participants stated that in all work items that are considered critical by the agile development team, the team defines the privacy principles that are related to the item, so that each one is implemented during the coding phase (RQ.3:Q1). This result confirms the findings of the survey, where 93% of work items from agile teams are critical to privacy and should be based on data protection objectives.

Regarding RQ.3: Q2, the focus group participants stated that deciding on a fixed set of privacy requirements can compromise the software development process. Participants stated that they use UML documents to register some stages of the development process and that these documents facilitate privacy requirements elicitation (RQ.3: Q3). In addition, the participants stated that data model and class diagram allow capturing information related to user privacy, which facilitates the documentation of privacy requirements (RQ.3:Q4). This result confirms the findings of the survey, where 60% of agile teams agree that data model or class diagram can be used as part of the iterative workflow to retain accurate privacy information.

According to the focus group participants, privacy criteria are usually elicited using a user story. Thus, for each privacy criteria, a scenario is described through a user story

(RQ.3:Q5), and this was confirmed for 79% of agile teams in the survey.

Summary: Work items are critical to privacy and should be based on data protection objectives. Data model or class diagram can be used as part of the iterative workflow to retain accurate privacy information. For each privacy criteria, a scenario is described through a user story.

Regarding RQ.3:Q6, some participants mentioned:

" *I think my biggest difficulty is identifying which items in the user story are related to privacy principles. In addition, user stories are almost always out of date and do not include the evolution of requirements. I think the biggest difficulties are related to consent, because we don't know how to insert privacy criteria in the development process.***"**

" *I think it is the knowledge of the legal aspects on the part of requirements analysts and stakeholders. In addition, I think we have a hard time eliciting privacy requirements, because data is often found in market tools or legacy systems.***"**

Regarding RQ.3:Q7, some participants suggested using the following practices:

"*Agile teams should prepare a detailed checklist using simple language to present to stakeholders, discussing the reasons and applications of the data privacy principles. In addition, they must use privacy by default.***"**

"*Agile teams should use Design Thinking techniques and tools in privacy requirements elicitation, during the early stages of the development process, using aspects of the law, technological and functional requirements. The implementation of data privacy must be done by the development team, mainly in relation to technical aspects, using data encryption, anonymization, etc. However, the demands related to LGPD must be dealt with at the organizational level and must be more of a type of requirements solicited by the requesting areas.***"**

Summary: Some practices adopted and difficulties mentioned by agile teams were common, both in the survey and in the focus group, for example, Lack of knowledge of the law by developers and users, and difficulty with documentation and accountability. Privacy should be the responsibility of developers and the principles of the LGPD must be treated separately.

V. Limitations and Threats to Validity

We cannot guarantee that all primary studies related to privacy requirements elicitation in the context of agile software development have been selected in the execution of the systematic literature review. To mitigate this threat, three researchers conducted searches on the digital databases that were established. However, we cannot guarantee that all studies were selected.

An important limitation to the results of this research is that we evaluated agile teams' perceptions of LGPD's impact on their daily activities, however, we did not evaluate the effects on the development of a real software – a product developed by agile teams – that actually comply with the data privacy regulations imposed by LGPD. This means that, if they state that LGPD will impact their work in any way, it is their perceptions, but not necessarily the reality, since is not yet demanded by control authorities the compliance of software developed by Brazilian organizations. Nonetheless, the focus of this research is on agile team perceptions rather than direct observations. Measuring perceptions of agile teams after the law comes into effect will be important in finding the real impact of LGPD on the execution of agile team activities. Another threat is that the focus group was conducted by one of the co-authors of this paper and it may have induced participants' responses. As a way to mitigate this threat, the first author performed an analysis of the results obtained in conjunction with the moderator, so that there was no bias regarding the conclusion of the participants' perception. In addition, interviews were conducted with all participants together, which could be a threat to validity. We could not interview each participant separated due to the limited time they have conceded.

VI. Conclusions

This paper investigated the perception of agile teams regarding the impacts of LGPD on agile software development activities. We conducted a survey in which participants answered various privacy related questions. To complement information obtained, we also conducted a focus group with experienced professionals from a public agency responsible for federal government security. It was possible to conclude from the survey results that agile teams are aware and are already working with some of the privacy principles, as well as adopting privacy solutions consolidated by the literature. In addition, most agile teams think that the organizational environment can interfere with privacy practices and that organizations should improve their organizational policy by clearly stating privacy and information security issues, and disclosing to all their members the policy adopted by them.

An important finding is that agile teams consider outdated user stories a threat to the proper implementation of data privacy and that privacy requirements must be detailed in its entirety in a user story or use case. In addition, most agile teams adopt the Scrum methodology. As future work, we intend to conduct a survey with agile teams from various organizations after LGPD implementation so that we can

compare the results with this research, to get perceptions of agile teams before and after the law gets effect, once organizations should develop their systems in compliance with the LGPD.

REFERENCES

[1] G. D. P. Regulation, "Eu data protection rules," *European Commission, Accessed in October 9, 2019*, 2018. [Online]. Available: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[2] P. da República, "Lei geral de proteção de dados pessoais (lgpd)," *Secretaria-Geral, accessed in October 9, 2019*, 2018. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

[3] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Methods for designing privacy aware information systems: A review," in *Panhellenic Conference on Informatics*. IEEE Computer Society, 2009, pp. 185–194.

[4] K. Thomas, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Distilling privacy requirements for mobile applications," in *36th International Conference on Software Engineering, ICSE '14, Hyderabad, India - May 31 - June 07, 2014*, 2014, pp. 871–882. [Online]. Available: https://doi.org/10.1145/2568225.2568240

[5] I. Hadar, T. Hasson, O. Ayalon, E. Toch, M. Birnhack, S. Sherman, and A. Balissa, "Privacy by designers: software developers' privacy mindset," *Empirical Software Engineering*, vol. 23, no. 1, pp. 259–289, 2018. [Online]. Available: https://doi.org/10.1007/s10664-017-9517-1

[6] R. Balebako, A. Marsh, J. Lin, J. Hong, and L. Cranor, "The privacy and security behaviors of smartphone," in *Workshop on Usable Security (USEC 2014), San Diego, 2014*, 2014.

[7] A. De Lucia and A. Qusef, "Requirements engineering in agile software development," *Journal of Emerging Technologies in Web Intelligence*, vol. 2, no. 3, pp. 212–220, 2010.

[8] B. Ramesh, L. Cao, and R. Baskerville, "Agile requirements engineering practices and challenges: an empirical study," *Inf. Syst. J.*, vol. 20, no. 5, pp. 449–480, 2010.

[9] M. Younas, D. Jawawi, I. Ghani, and R. Kazmi, "Non-functional requirements elicitation guideline for agile methods," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 3-4, pp. 137–142, 2017.

[10] S. Wagner, D. M. Fernández, M. Felderer, A. Vetrò, M. Kalinowski, R. J. Wieringa, D. Pfahl, T. Conte, M. Christiansson, D. Greer, C. Lassenius, T. Männistö, M. Nayebi, M. Oivo, B. Penzenstadler, R. Prikladnicki, G. Ruhe, A. Schekelmann, S. Sen, R. O. Spínola, A. Tuzcu, J. L. de la Vara, and D. Winkler, "Status quo in requirements engineering: A theory and a global family of surveys," *ACM Trans. Softw. Eng. Methodol.*, vol. 28, no. 2, pp. 9:1–9:48, 2019.

[11] S. Easterbrook, J. Singer, M. D. Storey, and D. E. Damian, "Selecting empirical methods for software engineering research," in *Guide to Advanced Empirical Software Engineering*. Springer, 2008, pp. 285–311.

[12] A. Meier and M. Kropp, "Swiss agile study – agile und hybride software-entwicklung in der schweiz," Swiss Agile Research Network, http://www.swissagilestudy.ch/files/2017/09/3.SwissAgileStudy.pdf, Tech. Rep., 2017.

[13] V. Inc., "14th state of agile report, tech. rep." Digital.ai Software, https://explore.digital.ai/state-of-agile/14th-annual-state-of-agile-report, Tech. Rep., 2020.

[14] M. A. G. Darrin and W. S. Devereux, "The agile manifesto, design thinking and systems engineering," in *2017 Annual IEEE International Systems Conference, SysCon 2017, Montreal, QC, Canada, April 24-27, 2017*, 2017, pp. 1–5. [Online]. Available: https://doi.org/10.1109/SYSCON.2017.7934765

[15] K. Beck, M. Beedle, A. van Bennekum, A. Cockburn, W. Cunningham, M. Fowler, J. Grenning, J. Highsmith, A. Hunt, R. Jeffries, J. Kern, B. Marick, R. C. Martin, S. Mellor, K. Schwaber, J. Sutherland, and D. Thomas, "Manifesto for agile software development," agilemanifesto.org/, Tech. Rep., 2001. [Online]. Available: https://agilemanifesto.org/

[16] O. Cawley, X. Wang, and I. Richardson, "Lean/agile software development methodologies in regulated environments - state of the art," in *Lean Enterprise Software and Systems - First International Conference, LESS 2010, Helsinki, Finland, October 17-20, 2010. Proceedings*, 2010, pp. 31–36. [Online]. Available: https://doi.org/10.1007/978-3-642-16416-3_4

[17] I. Sommerville, *Software engineering, 8th Edition*, ser. International computer science series. Addison-Wesley, 2007. [Online]. Available: http://www.worldcat.org/oclc/65978675

[18] M. Kassab, "The changing landscape of requirements engineering practices over the past decade," in *2015 IEEE Fifth International Workshop on Empirical Requirements Engineering, EmpiRE 2015, Ottawa, ON, Canada, August 24, 2015*, 2015, pp. 1–8. [Online]. Available: https://doi.org/10.1109/EmpiRE.2015.7431299

[19] V. T. Heikkilä, D. E. Damian, C. Lassenius, and M. Paasivaara, "A mapping study on requirements engineering in agile software development," in *41st Euromicro Conference on Software Engineering and Advanced Applications, EUROMICRO-SEAA 2015, Madeira, Portugal, August 26-28, 2015*, 2015, pp. 199–207. [Online]. Available: https://doi.org/10.1109/SEAA.2015.70

[20] E. Schön, J. Thomaschewski, and M. J. Escalona, "Agile requirements engineering: A systematic literature review," *Computer Standards & Interfaces*, vol. 49, pp. 79–91, 2017. [Online]. Available: https://doi.org/10.1016/j.csi.2016.08.011

[21] S. Gurses and J. M. del Álamo, "Privacy engineering: Shaping an emerging field of research and practice," *IEEE Security & Privacy*, vol. 14, no. 2, pp. 40–46, 2016. [Online]. Available: https://doi.org/10.1109/MSP.2016.37

[22] S. É. R. Ferrão, A. P. Carvalho, E. D. Canedo, A. P. B. Mota, P. H. T. Costa, and A. J. Cerqueira, "Diagnostic of data processing by brazilian organizations - A low compliance issue," *Inf.*, vol. 12, no. 4, p. 168, 2021.

[23] E. D. Canedo, A. J. Cerqueira, R. M. Gravina, V. C. Ribeiro, R. Camões, V. E. dos Reis, F. L. L. de Mendonça, and R. T. de Sousa Jr., "Proposal of an implementation process for the brazilian general data protection law (LGPD)," in *ICEIS (1)*. SCITEPRESS, 2021, pp. 19–30.

[24] B. ISO, "Iec 29100, 2011. bs iso/iec29100: Information technology—security techniques—privacy framework," Technical report, British Standard and the International Organization for ..., Tech. Rep., 2011.

[25] V. Ayala-Rivera and L. Pasquale, "The grace period has ended: An approach to operationalize GDPR requirements," in *RE*. IEEE Computer Society, 2018, pp. 136–146.

[26] D. by OneTrust, "Comparing privacy laws: Gdpr versus lgpd," *DataGuidance by OneTrust, Accessed in October 9, 2019*, 2019. [Online]. Available: https://www.dataguidance.com/comparing-privacy-laws-gdpr-v-lgpd/

[27] E. D. Canedo, A. T. S. Calazans, E. T. S. Masson, P. H. T. Costa, and F. Lima, "Perceptions of ICT practitioners regarding software privacy," *Entropy*, vol. 22, no. 4, p. 429, 2020.

[28] P. N. Otto and A. I. Antón, "Addressing legal requirements in requirements engineering," in *15th IEEE International Requirements Engineering Conference, RE 2007, October 15-19th, 2007, New Delhi, India*, 2007, pp. 5–14. [Online]. Available: https://doi.org/10.1109/RE.2007.65

[29] K. Bednar, S. Spiekermann, and M. Langheinrich, "Engineering privacy by design: Are engineers ready to live up to the challenge?" *Inf. Soc.*, vol. 35, no. 3, pp. 122–142, 2019. [Online]. Available: https://doi.org/10.1080/01972243.2019.1583296

[30] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the pris method," *Requir. Eng.*, vol. 13, no. 3, pp. 241–255, 2008. [Online]. Available: https://doi.org/10.1007/s00766-008-0067-3

[31] M. F. Dennedy, J. Fox, and T. Finneran, *The privace engineer's manifest*. Apress open, 2014.

[32] M. Peixoto, C. Silva, R. Lima, J. Araújo, T. Gorschek, and J. Silva, "Pcm tool: privacy requirements specification in agile software development," in *Anais Estendidos da X Conferência Brasileira de Software: Teoria e Prática*. SBC, 2019, pp. 108–113.

[33] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requir. Eng.*, vol. 16, no. 1, pp. 3–32, 2011. [Online]. Available: https://doi.org/10.1007/s00766-010-0115-7

[34] S. Islam, H. Mouratidis, C. Kalloniatis, A. Hudic, and L. Zechner, "Model based process to support security and privacy requirements engineering," *IJSSE*, vol. 3, no. 3, pp. 1–22, 2012. [Online]. Available: https://doi.org/10.4018/jsse.2012070101

[35] C. Bartolini, S. Daoudagh, G. Lenzini, and E. Marchetti, "Gdpr-based user stories in the access control perspective," in *Quality of Information and Communications Technology - 12th International Conference, QUATIC 2019, Ciudad Real, Spain, September 11-13, 2019, Proceedings*, 2019, pp. 3–17. [Online]. Available: https://doi.org/10.1007/978-3-030-29238-6_1

[36] H. Rygge and A. Jøsang, "Threat poker: Solving security and privacy threats in agile software development," in *NordSec*, ser. Lecture Notes in Computer Science, vol. 11252. Springer, 2018, pp. 468–483.

[37] B. A. Kitchenham, P. Brereton, M. Turner, M. Niazi, S. G. Linkman, R. Pretorius, and D. Budgen, "Refining the systematic literature review process - two participant-observer case studies," *Empirical Software Engineering*, vol. 15, no. 6, pp. 618–653, 2010.

[38] V. Wilson, "Research methods: triangulation," *Evidence based library and information practice*, vol. 9, no. 1, pp. 74–75, 2014.

[39] U. Flick, *An introduction to qualitative research*. Sage Publications Limited, 2018.

[40] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," *Department of Computer Science University of Durham Durham,UK*, 2007.

[41] M. M. Peixoto, "Privacy requirements engineering in agile software development: a specification method," in *REFSQ Workshops*, ser. CEUR Workshop Proceedings, vol. 2584. CEUR-WS.org, 2020.

[42] K. Curcio, T. Navarro, A. Malucelli, and S. S. Reinehr, "Requirements engineering: A systematic mapping study in agile software development," *J. Syst. Softw.*, vol. 139, pp. 32–50, 2018.

[43] L. Zamudio, J. A. Aguilar, C. T. Barba, and S. Misra, "A requirements engineering techniques review in agile software development methods," in *ICCSA (5)*, ser. Lecture Notes in Computer Science, vol. 10408. Springer, 2017, pp. 683–698.

[44] M. Viitaniemi, "Privacy by design in agile software development," Master's thesis, Master's Degree Programme in Information Technology, Tampere University of Technology, 2017.

[45] K. Loser and M. Degeling, "Security and privacy as hygiene factors of developer behavior in small and agile teams," in *HCC*, ser. IFIP Advances in Information and Communication Technology, vol. 431. Springer, 2014, pp. 255–265.

[46] T. J. Wagner and T. C. Ford, "Metrics to meet security & privacy requirements with agile software development methods in a regulated environment," in *International Conference on Computing, Networking and Communications, ICNC 2020, Big Island, HI, USA, February 17-20, 2020*, 2020, pp. 17–23. [Online]. Available: https://doi.org/10.1109/ICNC47757.2020.9049681

[47] A. T. S. Calazans, A. J. Cerqueira, and E. D. Canedo, "Empathy and criativity in privacy requirements elicitation: Systematic literature review," in *WER*. Editora PUC-Rio, 2020.

[48] I. Oliver, "Experiences in the development and usage of a privacy requirements framework," in *24th IEEE International Requirements Engineering Conference, RE 2016, Beijing, China, September 12-16, 2016*, 2016, pp. 293–302. [Online]. Available: https://doi.org/10.1109/RE.2016.59

[49] Y. Katsuno, A. Kundu, K. K. Das, H. Takahashi, R. Schloss, P. Dey, and M. K. Mohania, "Security, compliance, and agile deployment of personal identifiable information solutions on a public cloud," in *9th IEEE International Conference on Cloud Computing, CLOUD 2016, San Francisco, CA, USA, June 27 - July 2, 2016*, 2016, pp. 359–366. [Online]. Available: https://doi.org/10.1109/CLOUD.2016.0055

[50] R. Galvez and S. Gurses, "The odyssey: Modeling privacy threats in a brave new world," in *2018 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2018, London, United Kingdom, April 23-27, 2018*, 2018, pp. 87–94. [Online]. Available: https://doi.org/10.1109/EuroSPW.2018.00018

[51] K. Rindell, S. Hyrynsalmi, and V. Leppänen, "Aligning security objectives with agile software development," in *Proceedings of the 19th International Conference on Agile Software Development, XP 2019, Companion, Porto, Portugal, May 21-25, 2018*, 2018, pp. 3:1–3:9. [Online]. Available: https://doi.org/10.1145/3234152.3234187

[52] A. van der Heijden, C. Broasca, and A. Serebrenik, "An empirical perspective on security challenges in large-scale agile software development," in *Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, ESEM 2018, Oulu, Finland, October 11-12, 2018*, 2018, pp. 45:1–45:4. [Online]. Available: https://doi.org/10.1145/3239235.3267426

[53] P. Maier, Z. Ma, and R. Bloem, "Towards a secure SCRUM process for agile web application development," in *Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, August 29 - September 01, 2017*, 2017, pp. 73:1–73:8. [Online]. Available: https://doi.org/10.1145/3098954.3103171

[54] D. Netto, C. Silva, and J. Araújo, "Identifying how the brazilian software industry specifies legal requirements," in *Proceedings of the XXXIII Brazilian Symposium on Software Engineering, SBES 2019, Salvador, Brazil, September 23-27, 2019*, 2019, pp. 181–186. [Online]. Available: https://doi.org/10.1145/3350768.3352730

[55] N. Newton, C. Anslow, and A. Drechsler, "Information security in agile software development projects: a critical success factor perspective," in *ECIS*, 2019.

[56] I. A. Tøndel, D. S. Cruzes, M. G. Jaatun, and K. Rindell, "The security intention meeting series as a way to increase visibility of software security decisions in agile development projects," in *ARES*. ACM, 2019, pp. 59:1–59:8.

[57] D. Ionita, C. van der Velden, H. K. Ikkink, E. Neven, M. Daneva, and M. Kuipers, "Towards risk-driven security requirements management in agile software development," in *CAiSE Forum*, ser. Lecture Notes in Business Information Processing, vol. 350. Springer, 2019, pp. 133–144.

[58] I. A. Tøndel, M. G. Jaatun, D. S. Cruzes, and L. Williams, "Collaborative security risk estimation in agile software development," *Inf. Comput. Secur.*, vol. 27, no. 4, 2019.

[59] K. Bernsmed and M. G. Jaatun, "Threat modelling and agile software development: Identified practice in four norwegian organisations," in *Cyber Security*. IEEE, 2019, pp. 1–8.

[60] E. D. Canedo, A. T. S. Calazans, A. J. Cerqueira, P. H. T. Costa, and E. T. S. Masson, "Using the design thinking empathy phase as a facilitator in privacy requirements elicitation," in *AMCIS*. Association for Information Systems, 2020.

[61] J. Kontio, L. Lehtola, and J. Bragge, "Using the focus group method in software engineering: obtaining practitioner and user experiences," in *Empirical Software Engineering, 2004. ISESE'04. Proceedings. 2004 International Symposium on*. IEEE, 2004, pp. 271–280.

[62] M. Alsaadi, A. Lisitsa, M. Khalaf, and M. Qasaimeh, "Investigating the capability of agile processes to support medical devices regulations: The case of xp, scrum, and FDD with EU MDR regulations," in *ICIC (3)*, ser. Lecture Notes in Computer Science, vol. 11645. Springer, 2019, pp. 581–592.

[63] V. G. Ferreira and E. D. Canedo, "Using design sprint as a facilitator in active learning for students in the requirements engineering course: an experience report," in *SAC*. ACM, 2019, pp. 1852–1859.

[64] R. dos Santos Braz, J. R. Merlin, D. de Freitas Guilhermino Trindade, C. E. Ribeiro, E. M. Sgarbi, and F. de Sordi Junior, "Design thinking and scrum in software requirements elicitation: A case study," in *HCI (18)*, ser. Lecture Notes in Computer Science, vol. 11583. Springer, 2019, pp. 179–194.

[65] N. Tripathi, M. Oivo, K. Liukkunen, and J. Markkula, "Startup ecosystem effect on minimum viable product development in software startups," *Information & Software Technology*, vol. 114, pp. 77–91, 2019.

[66] E. del Nuevo, M. Piattini, and F. J. Pino, "Scrum-based methodology for distributed software development," in *ICGSE*. IEEE Computer Society, 2011, pp. 66–74.

[67] O. Ayalon, E. Toch, I. Hadar, and M. Birnhack, "How developers make design decisions about users' privacy: The place of professional communities and organizational climate," in *CSCW Companion*. ACM, 2017, pp. 135–138.