TSOHOU, A., MAGKOS, E., MOURATIDIS, H., CHRYSOLORAS, G., PIRAS, L., PAVLIDIS, M., DEBUSSCHE, J., ROTOLONI, M. and CRESPO, B. G.-N. 2020. Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. *Information and computer security* [online], 28(4), pages 531-553. Available from: https://doi.org/10.1108/ICS-01-2020-0002

Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform.

TSOHOU, A., MAGKOS, E., MOURATIDIS, H., CHRYSOLORAS, G., PIRAS, L., PAVLIDIS, M., DEBUSSCHE, J., ROTOLONI, M. and CRESPO, B. G.-N.

2020

Privacy, Security, Legal and Technology Acceptance Elicited and Consolidated Requirements for a GDPR Compliance Platform

Abstract.

Purpose: GDPR entered into force in May 2018 for enhancing personal data protection. Even though GDPR leads towards many advantages for the data subjects it turned out to be a significant challenge. Organizations need to implement long and complex changes to become GDPR compliant. Data subjects are empowered with new rights, which however they need to become aware of. GDPR compliance being a challenging matter for the relevant stakeholders calls for a software platform that can support their needs. The aim of the Data govErnance For supportiNg gDpr (DEFeND) EU Project is to deliver such a platform. In this paper, we describe the process, within the DEFeND EU Project, for eliciting and analyzing requirements for such a complex platform.
Design/methodology/approach: The platform needs to satisfy legal and privacy requirements and provide functionalities that data controllers request for supporting GDPR compliance. Further, it needs to satisfy acceptance requirements, for assuring that its users will embrace and use the platform. In this paper, we describe the methodology for eliciting and analyzing requirements for such a complex platform, by analyzing data attained by stakeholders from different sectors.
Findings: Our findings provide the process for the DEFeND platform requirements' elicitation and an indicative sample of those. We also describe the implementation of a secondary process for consolidating the elicited requirements into a consistent set of platform requirements.
Research/Practical implications: The proposed software engineering methodology and data collection tools (i.e., questionnaires) are expected to have significant impact for software engineers in the academia and industry.
Social implications: It is reported repeatedly that data controllers face difficulties in complying with the GDPR. Our work aims to offer mechanisms and tools that can assist organizations to comply with the GDPR, thus offering significant boost towards the European personal data protection objectives.
Originality/value: This is the first paper to provide software requirements for a GDPR compliance platform, including multiple perspectives.

Keywords: GDPR, compliance, software requirements, prioritization, consolidation.

1 Introduction

Since May 2018 the General Data Protection Regulation (GDPR) has become the center of attention for practitioners, researchers, governments, and citizens. The General Data Protection Regulation enforces significant changes on the way that personal data is being processed, the way that data protection authorities guide and audit data controllers and on the individual rights of data subjects. Further, GDPR altered the territorial scope of the European Data Protection framework, enforcing changes to service providers who serve data subjects living in European member states.

For entities that process personal data (i.e., data controllers or data processors) the enforcement of GDPR means the implementation of organizational and technical changes, including the deployment of tools that allow demonstration of GDPR compliance, the appointment of Data Protection Officers, the conduction of privacy impact assessments, the training of staff, the implementation of data de-identification techniques, and so on. According to the first official report on implementation of the GDPR, provided by the European Data Protection Board (European Data Protection Board, 2019), most organizations have increased their financial budget allocated to personal data protection (30%-50%), increased the personnel allocated, while a total of 206.326 legal cases have been presented to the authorities from 31 member states (complaints, data breaches, etc.). Thomson Reuters (2019) reports that organizations are still not ready in terms of GDPR compliance, and many of them know very little about the Regulation and whether or how it will affect them. A report by ISACA also presents a similar view (approximately 65% of organizations reported not ready in terms of GDPR compliance in May 2018) and elaborates on the technical, regulatory and legislative tools that should be implemented to assist organizations in their compliance efforts (ISACA, 2019).

We aim to address this research and industrial gap through the development of a GDPR compliance platform that will deliver tools for organizations and interfaces for data protection authorities and citizens to interact with the organizations that process personal data. We do so, through the Data govErnance For supportiNg gDpr (DEFeND) EU Project (www.defendproject.eu/) that is dedicated into delivering such a platform (the concept is also described in Piras et al., 2019). Ten organizations collaborate for the provision of the platform from Spain, UK, Italy, Portugal, Bulgaria, Greece and France. The DEFeND platform will guide organizations in fulfilling GDPR compliance through Privacy by Design and by Default tools, and in supporting consent management, privacy analysis, security risk assessment, and data breach management. The platform will also support citizens concerning personal data management, awareness and breach notifications. Finally, it will support the interaction of organizations with the respective data protection authorities.

In this paper, we extend the software engineering methodology that was presented in earlier work (Authors names removed for review) and describe the results capturing the needs of users and modeling the software requirements for a GDPR Compliance Platform. Our software engineering approach spanned into multiple aspects of user needs, including functional, security, privacy, legal and acceptance requirements. We

collected user needs focusing on four industrial sectors; namely financial, health, public administration and energy management. We emphasize on the financial sector and the respective lessons learned. Following the primary data analysis to extract software requirements per distinct need (e.g., functional, legal) which was described in earlier work (Authors names removed for review), in this extended paper we describe the secondary analysis through which we achieved the consolidation of the various requirements into a consistent set of platform requirements.
The paper is structured into seven sections. Following this introduction, section 2 provides a review of state of the art to reveal the industrial and academic needs associated with a GDPR compliance platform. Section 3 presents our software engineering approach and Section 4 presents our methodology to collect data for capturing software requirements. Section 5 presents indicative software requirements that resulted from the primary process and Section 6 presents the secondary process for the consolidation of the initial requirements. Section 7 provides the knowledge that was learnt from this process and could be informative for similar endeavors. Finally, Section 8 concludes the paper.

2 The Defend Project and its Position in the Industry and Society

2.1 Industry State of the Art

The evolution of European organizations' readiness for GDPR compliance before May 25, 2018 until today shows that, although there is significant progress achieved since that date, there is still a long way to go. A recent research report by TrustArc (2018) shows that 27% of the organizations in Europe (excluding the UK), 21% in the UK and 12% in the U.S. reported believing to be compliant. These numbers show a significant increase in comparison to the situation in 2017 and the research report forecast is that 93% of the companies expect to be compliant by the end of 2019.
Organizational compliance towards GDPR is expected to impact in significant expenditures. A PwC survey, conducted in 2016, predicted that 40% of large organization will spend more than 10 million dollars on GDPR compliance (Pulse Survey, 2016). Also, Gartner (2017) predicted that 65% of all data loss prevention buying decisions will be driven by GDPR through 2018. The situation one year after, as described by the participants in TrustArc's report shows that 68% of the organizations already have spent more than six figures on GDPR compliance and 67% expect to spend an additional six figures by the end of 2018 in order to reach full compliance.
Investing in technology has become a popular strategy among companies in Europe to achieve compliance with regulations such as the Data Protection Directive (95/46) and EU's General Data Protection Regulation. According to TrustArc's report, 87% of the companies assessed needed third party support and 94% used technology to help them in their GDPR implementation projects. There are many products already in the market that support organizations in managing their privacy requirements and

according to IAPP (2018), the number of vendors providing privacy management technologies has doubled in one year and some of the existing ones have enhanced their offering with new services. Despite the remarkable increase in the market offering, the report also highlights that "there is no single vendor that will automatically make an organization GDPR compliant".

2.2 Literature State of the Art

The DEFeND Platform will be contribute in research gaps spanning three axes of privacy protection, all related to the general obligations for controllers and processors for GDPR compliance.

Privacy by Design (PbD). Data should be protected by design and by default (ar. 25, GDPR), in the sense that privacy should be proactively adopted, be embedded into the design phase of new systems and services, and also be enforced as a default setting (Cavoukian, 2011; Kurtz & Semmann, 2018; Bednar et al., 2019). While a number of methodologies for privacy by design have been proposed during the last decade (e.g., (Kalloniatis et al., 2011; Deng et al., 2011; Faßbender et al., 2014; Notario et al., 2015), recent surveys (e.g., (Danezis et al., 2015; Kurtz & Semmann, 2018)) exhibit a lack of technologies and/or tools to implement the PbD principle in a holistic way. Indeed, except for a small number of paradigms, where the articles of the GDPR are integrated early in the development steps (e.g., Vanezi et al, 2019), PbD principles have not yet gained adoption in the engineering practice, mainly because a mismatch between the legal and technological mindsets (Martin & Kung, 2018, Horák et al, 2019) with the result being that engineers are mostly relied on privacy policies for compliance. The DEFeND project advances state-of-the-art by facilitating organisations to implement a privacy management approach that takes into account the PbD principles, enabling them to (re)design their processes with respect to their privacy requirements, at an operational level (Piras et al., 2019).

Consent Management. Until recently, users were supposed to read privacy policies or notices before giving their consent to the data controller for processing their data, but in reality users never read them (McDonald & Cranor, 2008). The cost of reading privacy policies. ISJLP, 4, 543.), in which case consent becomes not informed (Tsohou & Kosta, 2017). Even if the users read the privacy policies, it is usually difficult to follow the legal and technical terminology inside (often, lengthy) policy texts and notices. With GDPR's more strict requirements on: (a) the consent being specific; (b) getting parents' consent for processing children data; (c) respecting data subjects' rights to revoke their consent, technologies and tools should provide users the possibility to withdraw consent as easily as they gave it. State of the art technologies and/or tools to implement the Lawfulness of Processing (ar. 6, GDPR) principle in a holistic way do not exist or are still immature (Politou et al., 2018; Priyadharshini & Shyamala, 2018; Li et al, 2019). The DEFeND project approaches consent management in a holistic way, delivering a Privacy Data Consent (PDC) to users which will act as a contract among the data controller and data subject, encapsulating all the necessary information regarding the consent of the processing to their personal data.

Privacy Impact Assessment (PIA). The execution of PIAs (ar. 35, GDPR) should ideally be supported by an information security risk management system to identify and reduce the privacy risks of data subjects when their personal data are processed by data controllers. Given that the guidelines of ISO/IEC 27005:2011 do not include PIAs, and that data protection standards such as BS 10012:2017, ISO/IEC 29151:2017, ISO/IEC 27018:2014, require PIA in addition to conducting information security risk assessments, in 2017 ISO issued the ISO/IEC 29134:2017 standard with guidelines for PIA, superseding ISO 22307:2008 ("Financial services - Privacy impact assessment") and related guidelines (WP29 Guidelines on Data Protection Impact Assessment, 2017). In addition, apart from a handful of notable exceptions (e.g., Horák et al, 2019), state of the art methodologies and tools to implement PIA are still immature (Bisztray & Gruschka, 2019) and there is a lack of DPIA methodologies to investigate the risks of information sharing in software engineering practice under the new requirements imposed by GDPR.. The DEFeND platform will advance the current state of the art in Data Protection Impact Assessment by providing an in-depth processing analysis based on a recognized methodology and international standards.

The DEFeND Platform aims to support organisations towards GDPR compliance allowing however adaptability so that organizations can choose which modules they wish to use and/or extend. The platform is founded in a model that spans over two levels, the Planning Level and the Operational Level, and across three management areas, i.e. Data Scope, Data Process and Data Breach. More information about the DEFeND platform architecture and design can be found at the project's website (www.defendproject.eu/) and the description of the platform concept in Piras at al. (2019).

3 A Holistic Engineering Approach: Functional, Privacy, Security, Legal and Acceptance Needs

3.1 Stakeholder Analysis

A stakeholder is an entity that can be influenced by the results of the DEFeND project. In this task we were interested on key stakeholders possibly engaged and committed to use the DEFeND platform, i.e., operate or depend on it. Different DEFeND users may have different expectations on the functionalities of the DEFeND platform, the services and support which will be provided, as well as on the importance of the security and privacy aspects of the GDPR compliance (e.g., for a citizen's role, breach notification and managing user consent) and the visualization of such compliance within the platform. The consortium identified the possible users in different scenarios and classified them, according to their types:

a) Internal Stakeholders: Stakeholders who are responsible for activities regarding the GDPR compliance in an organization, such as Data Protection Officer (DPOs), CEOs, CIOs, IT managers, Risk Assessment Officers, Audit Officers. Data Protection Officers (DPOs), in organizations who have appointed one, represented the

best role to answer the questionnaire; however, within each organization different roles might be responsible for the actions for compliance with the GDPR.

a) External Stakeholders: External stakeholders included *citizens* as data subjects when interacting with industry providers (i.e., in the health, banking, energy or public administration sectors), as we all *supervisory authorities.* The functional requirements for the supervisory authorities are mostly described by GDPR itself.

3.2 Privacy and Security Needs

For the identification of privacy and security needs we utilized state-of-the-art security requirements engineering methodologies (Dubois and Mouratidis, 2010) on top of modeling languages and methodologies and tools for security by design and privacy by design that partners have performed, such as the Secure Tropos (Mouratidis & Giorgini, 2007; Mouratidis, 2011; Islam et al., 2012) security-aware software systems development methodology and related tool (SecTro (Pavlidis et al., 2012; Pavlidis & Islam, 2011)). These were used to elicit, model and analyse the privacy and security requirements of the GDPR platform and were extended to include human factors during the privacy/security requirements engineering level. The resulted tools will support organisations in understanding security and privacy requirements, and design systems and services that fulfill those requirements.

3.3 Legal Needs

Building a platform for GDPR compliance necessarily requires evaluating all aspects from a legal perspective. Indeed, any tool or functionality of a particular GDPR compliance platform, including the DEFeND platform, needs to be assessed in light of the specific requirements imposed by the legislation (i.e. the GDPR). This necessitated a careful evaluation of each relevant article, including of its conditions and exceptions, and the interaction it may have with other articles and Recitals of the GDPR. Failing to perform such investigation of the legal requirements would lead to building a platform that would not sufficiently encapsulate the obligations enshrined in the GDPR and thus be incomplete or inaccurate.

3.4 Technology Acceptance Needs

Acceptance requirements are non-functional requirements that consider psychological, cognitive, sociological factors to take into account for individuating strategies stimulating the user to accept to use a software system, particular system features or new technological methods (Piras, 2018; Piras et al., 2016, 2017, 2017b, 2019). In fact, it happens often that, when the user starts using a new system, she has some difficulties, gets bored in relation to repetitive software tasks or due to complex procedures, and the result is that the user leaves the system. Therefore, in order to favor the acceptance and the usage of a system, acceptance requirements need to be considered and elicited starting from the early stages of any software engineering process by performing an acceptance requirements analysis. This is particularly

relevant here because the DEFeND platform is expected to serve the needs of different heterogeneous actors with different expertise, interests and motivations.

In order to decide how analyze the acceptance reequipments for the DEFeND platform, we reviewed the literature, and selected Agon as our requirements analysis framework given its acknowledgement in the requirements engineering community (Piras, 2018; Piras et al., 2016, 2017, 2017b, 2019). Agon supports acceptance requirements analysis and operationalizes those requirements throughusing game concepts and design mechanisms for improving software features. Agon supports the analyst in a systematic acceptance requirements analysis and design of gamification, by providing guidance and suggestions, with an interactive method (Piras, 2018; Piras et al., 2016, 2017b, 2019). Moreover, the effectiveness of Agon has been proved in many heterogeneous domains, in realistic and real cases within European Projects (Piras, 2018; Piras et al., 2017b, 2019). For these reasons, we employed the Agon framework for our acceptance requirements analysis for the DEFeND platform.

4 A Methodology to Elicit Software Requirements for a GDPR Compliance Platform

Towards defining the requirements necessary to be used as basis for building the DEFeND platform, we used a *Human-Centered design* (HCD), where incorporating the user's perspective into software development is considered of paramount importance in order to achieve a functional and usable system (Maguire, 2001). Based on widely accepted methodologies that have been proposed in the area of user-adaptive systems development, user data have been collected using *questionnaire-based* and *interviews-based* approaches in order to assist *the elicitation of requirements* for the platform. Further, focus groups were realized in order to validate the data collection instruments and the elicited requirements. We identified the *key stakeholders*, and for each user category, a questionnaire was prepared, aiming at capturing the user needs concerning various aspects; legal, functional, security, privacy and acceptance aspects. In sequence, user needs were translated into software requirements for all levels of the DEFeND platform (Piras et al., 2019), i.e., Data Scope Management (DSM), Data Process Management (DPM), and Data Breach management (DBM). The overall approach is depicted in Fig. 1.

Figure 1 should be placed here

4.1 Preparation of Questionnaires

In order to collect internal users' needs we developed a questionnaire[1] and a different questionnaire for external users[2]. We should note that both questionnaires were not constructed to develop or validate a theory (i.e., typical survey questionnaire process),

[1] https://ec.europa.eu/eusurvey/runner/DEFeNDEndUser
[2] https://ec.europa.eu/eusurvey/runner/DEFeNDCitizens

but instead it aims to captivate the questions that software analysts commonly ask in order to capture user needs, which will afterwards become translated into software functionalities. To discover and validate that we have identified the stakeholders' need(s), and thus build the right product to satisfy these need(s), we combined two approaches: First, we followed the approach established in (Blank, 2007) for customer development, which includes three main steps:

1. **Customer Segmentation.** A relevant action point was to consider the possibility of different questionnaire versions depending on the role of the internal stakeholder. In addition, each participant external stakeholder (i.e., citizen) completed the questionnaire having in mind only her personal data being processed by one sector (i.e., health organization or public administration or energy or bank organization). This was considered as important in order to register any number of different requirements per sector. Customer segmentation is supported by questionnaire's section regarding user information, questions 1-5 and background information, questions 6-15.
2. **Problem Discovery and Validation.** The second category of questions aimed at validating the hypotheses about the problem(s) and challenges that the DEFeND platform aims at dealing with, as depicted in DEFeND's proposal, but also at learning about new problems and challenges as conceived by the interviewees. This category is supported by questions 16-22.
3. **Product Discovery and Validation.** The third category of questions aims at validating the hypotheses about the usefulness of the specific features envisaged for the DEFeND platform, but also at learning about new features as conceived by the interviewees. This category is supported by questions 23-36, regarding features of an ideal GDPR tool, functional, privacy and security features of the DEFeND Platform, as well as usability, reliability and performance features.

Our second approach involved selecting questions that span over the two levels (planning and operational) and the three management areas (Data Scope Management, Data Process Management and Data Breach Management), to follow the Privacy by Design approach as envisaged by the project. To this end, questions included in the questionnaires for the interviews with both the end-users and citizens have been selected to depict the privacy-by-design approach and to capture the users' needs for the different components of the platform.

Additionally, during the preparation of the questionnaire we considered the necessity to derive acceptance requirements, using the Agon framework and method. Thus, we included in the questionnaires elements for collecting data regarding such aspects of the platform, i.e., relevant questions for characterizing the different DEFeND users (Piras, 2018; Piras et al., 2017b). In fact, the acceptance requirements analysis (Piras et al., 2016, 2017, 2017b) starts from the characterization of the user to motivate (Piras, 2018; Piras et al., 2019), by considering factors ranging from simple ones such as the age and gender information (Piras, 2018; Piras et al., 2016), to more complex ones such as the (i) difficulty of the task to be carried out by using the system, (ii) in which social structure will be used the system, (iii) characterization of the goal to be achieved, (iv) skills required for completing the task, (v) existing user knowledge related to previous usage of similar software systems (Piras, 2018; Piras et al., 2017),

etc. Therefore, we prepared a number of questions and included them in the different questionnaires, aiming at collecting such relevant information for the different stakeholders of the DEFeND platform.

4.2 Validation of Questionnaires

The initially prepared questionnaire was commented by ten DPOs working on the organizations that formulate the project consortium. The feedback was collected and processed by the technical partners to revise the questionnaire and the data collection process. In sequence we organized a focus group to discuss the revised questionnaire with internal stakeholders from the banking sector. The stakeholders held different roles on GDPR compliance (i.e., IT manager, DPOs, CIOs) and participated either to the focus group physically or online. The objective of this session was to gather feedback from the stakeholders on the revised questionnaire, regarding the structure, the expression of the questions, language and terms, etc. We should note that we shared the questionnaire with the participants ten days in advance, to allow sufficient preparation. The result of this stage was a consolidated draft of the questionnaire for the internal stakeholders (hereafter end users).

4.3 Data Collection Approach

We collected data regarding user needs from seven European countries (i.e., Italy, Greece, Spain, Bulgaria, France, Portugal, UK), spanning the two main stakeholder roles; organizations and citizens. Participants for organizational needs were individuals responsible for the coordination and monitoring of activities regarding the GDPR compliance. Citizens' needs were collected by any individual, since any identified or identifiable natural person is a data subject. In order to ensure that we gained insights into the understanding of multiple citizens' perspectives we targeted to include individuals with different characteristics (i.e., representation of males and females; of different age groups; of different education levels; of different GDPR awareness level). Given that many researchers were involved in the data collection and analysis process, we developed a data collection guidance document, which provided the steps to follow and necessary instructions. In order to ensure ethical principles, we developed an information participant sheet and a consent form the participants signed. Further, we provided a privacy policy that described our processing rules for the participants' personal data.

For organizational needs the data collection was conducted using semi-structured interviews and one online survey. The interviews were used to ensure in-depth analysis of needs of DPOs who are expected to be the main users of the platform. The online survey was utilized for the collection of needs from multiple stakeholders. For the online survey we used the EU Survey platform (https://ec.europa.eu/eusurvey/). For citizens' needs we used an online survey, using the same survey platform.

The interviews were semi-structured and were conducted based on an interview protocol. Semi-structured interviews use incomplete scripts, allowing for flexibility, improvisation, and openness (Myers & Newman, 2007). We also used the technique

of mirroring (Myers & Newman, 2007), according to which the interviewer uses the interviewees' words and phrases to construct subsequent questions.
For organizational needs we collected information from 10 individuals via interviews and 31 individuals via online survey, representing the energy, education, banking, health, public administration and information technology consultancy sectors. For citizens' needs we collected data from 174 individuals.

4.4 Data Analysis Approach

In order to elicit requirements from the data that were collected during the data collection phase, we followed a four iterative stage approach. The first 2 stages were held during a three-day workshop.
In the first stage, each working group analyzed collectively the responses resulting from the different numerical questions and from the open text contents. They deducted potential requirements for the DEFeND platform from these analyses. The resulting elicited requirements were aggregated into a single document acting as a first round of elicited requirements.
In the second stage, all partners acted as a single working group, reviewed the first round of requirements and refined them. This resulted in the second round of elicited requirements. The consortium during the first two stages used qualitative data analysis techniques and in particular open coding (Bryman, 2008; Juristo et al, 2006).
In the third stage, which was fulfilled through collaborative work partners we divided into various groups depending the type of requirements and their expertise. Regarding the end users' requirements, the technical partners of the consortium were divided into two working groups and each group was allocated with the responses corresponding to a level of the questionnaire (i.e., planning level, operational level). Regarding the citizens' requirements, the pilot partners of the consortium were allocated with analyzing the requirements resulting from the responses corresponding to five questions of the questionnaire. The above work resulted in the third round of elicited requirements.
In the fourth and final stage, the third round of elicited requirements was distributed to all partners for further refinement, resulting in the fourth round of elicited requirements.
During the first two stages the requirements were considered raw and acted as first level requirements. During the next two stages, the consortium agreed to follow a common way in expressing the requirements which was decided prior to the beginning of the third stage. The guidelines were as simple as possible in order to enable all partners, including non-technical ones, to give feedback. This approach allowed a consistent transformation of raw requirements. For example:

Raw requirement (stage 1 or 2):
"Dashboard showing overview of obligations and notifications to select which ones I want to be notified of", Question 25(d).
Refined requirement following consortium guidelines (stage 4):
Fun.REQ01.01: Platform shall utilize notifications on data breach.

Fun.REQ01.02: Citizens shall be able to customize preferences about breach notifications.

Regarding the closed ended questions, the consortium used the average value given by the participants for each question of the online questionnaires in order to prioritize the requirements.

5 Eliciting Requirements for a GDPR Compliance Platform

5.1 Functional and Privacy/Security Requirements

During the analysis of end users' needs at the planning level, a number of important outcomes were recorded:

- At the Data Scope Management area, most end users believed that a tool for data inventory and mapping would be the most critical and less difficult to achieve.
- At the Data Process Management area, end users believed that the most important features of a platform would be to allow them to review compliance activities and keep records for internal/external reporting to demonstrate compliance.
- At the Data Breach Management, most end users pointed out the criticality of a tool that allows them to define and review information security policies and incident response plans to comply with the GDPR obligations for reporting a breach.

During the analysis of stakeholders needs at the operational level, important outcomes included:

- At the Data Scope Management area, the assessment of organization's readiness for the GDPR was seen as the most important feature by the end users.
- At the Data Process Management area, the most important feature was to provide support for implementing security and privacy controls (e.g., anonymisation, encryption and authorisation).

During the analysis of citizens' needs, user-friendliness of the DEFeND platform and relevant interfaces was considered as mostly important, followed by the need to include a functionality that allows transparent management of users' consent.

Some indicative functional requirements are presented in Table 1.

Table 1 should be placed here

5.2 Legal Requirements

In terms of legal requirements, the DEFeND platform will offer to organizations several tools, components and functionalities to enable compliance with the numerous obligations imposed by the GDPR. In order to ensure that such tools, components and functionalities correspond to what is foreseen by the legal text of the GDPR, they need to be designed and developed on the basis of a list of legal privacy and security requirements. Accordingly, a list of requirements has been extracted and transposed on the basis of the legal text of the GDPR. The list of privacy and security legal

requirements is structured around the following 12 themes of the DEFeND platform (www.defendproject.eu/) The analysis relied on a desk research comprising of an analysis of the core legal text at the basis of the entire project (i.e. the GDPR), and of the 12 core themes of the DEFeND platform. In this context, a "privacy or security legal requirement" is to be understood as a single obligation extracted from one or more provisions of the GDPR that concern an organisation (i.e. a controller and/or processor), and which require that organisation either to do or to abstain from doing something in order to reach compliance or to document certain events or a reasoning to demonstrate compliance and which can be to a lesser or greater extent addressed through a technical solution corresponding to one or more of the 12 themes of the DEFeND Platform.

In order to define the privacy and security legal requirements, a thorough methodology has been followed, comprising of the following 7 steps. The first three steps of the methodology played an important role in determining which parts of the GDPR could be included or not in the DEFeND platform. Indeed, certain Chapters, Sections and Articles of the GDPR are not and cannot form part of a GDPR compliance platform due to their specific content or their purpose. Accordingly, the initial steps aimed to determine the relevance of each Chapter, Section and Article of the GDPR to the DEFeND Project. In order to determine such relevance, a three-step test composed of three cumulative criteria was applied. The first criterion related to the question whether the Chapter, Section or Article concerns an organisation (i.e. a controller and/or processor). The second criterion related to the question whether the Chapter, Section or Article requires the organisation either to do or to abstain from doing something or to document certain events or a reasoning to demonstrate compliance. The third and final criterion related to the question whether the Chapter, Section or Article corresponds to one or more of the 12 themes of the DEFeND Platform. Where all of the three criteria could be answered negatively for a particular Chapter, Section or Article it was concluded that it was not relevant to the DEFeND Project and therefore that no requirement could be extracted. Where the responses to at least one of the three criteria were (even partially) positive for a Chapter, we moved to step 2, in which the specific Sections of that Chapter were examined in terms of relevance applying the same three-step test. Where the responses to at least one of the three criteria were (even partially) positive for a Section, we moved to step 3, in which the individual Articles of that Section are examined in terms of relevance applying the same three-step test.

Figure 2 should be placed here

Ultimately, the project has identified concrete, practical privacy and security legal requirements that should ideally be met in relation to each theme of the DEFeND platform for it to be able to support organisations in complying with the GDPR. Considering both the 12 themes of the DEFeND platform and the GDPR requirements, 74 legal requirements have been compiled and distributed as depicted in Fig. 2.

Table 2 should be placed here

Some indicative legal requirements in the areas 'Developing a GDPR privacy plan' and 'Creating a third-party management program' are presented below in Table 2.

5.3 Technology Acceptance Requirements

The analysis of the questionnaire responses, in particular the questions targeting the elicitation of acceptance requirements (Piras, 2018; Piras et al., 2016, 2017, 2017b, 2019), provided us with information to identify the main characteristics and needs of the different users of the DEFeND platform to consider (Piras et al., 2019) as well as the users' characterization. For each type of DEFeND user we individuated psychological, cognitive, sociological factors and strategies to positively affect the user towards software acceptance. These requirements will help in designing and enhancing the DEFeND platform architecture, in a way that it can really support and motivate all the stakeholders (Piras, 2018; Piras et al., 2017b) to accept and use it. The elicited acceptance requirements will contribute to the development of the DEFeND platform in a way that for fulfils some of the important aspects the platform has to support, for instance: usability, ease of use, awareness of the framework and guidance provided to users.

As an example, we discovered that most of the citizens that will use the DEFeND platform will be males, young, socializers, not obliged to use the system (Piras, 2018; Piras et al., 2016), have not participated in the definition of the goal of the platform, it is enough clear the objective of the platform for them, and also why it could be useful for the user (Piras, 2017). Furthermore, they are not expert of this kind of software, have never used similar software, however their task in the usage of the platform do not require particular skills and tasks should be not very various for them (Piras, 2017). Moreover, they are interested in using the platform, they will use the platform in a social structure that is not hierarchical for producing benefits for themselves (Piras, 2017).

We have derived a number of acceptance requirements. For example, the citizen users of the DEFeND platform need to perceive the platform as useful and to see advantages in their usage helping them in guaranteeing the management of their personal data and that their rights are fulfilled. Furthermore, due to their characteristics and interests, they need to use the platform by interacting and collaborating in a social way with the other users, above all with people that can influence and help them, to receive at least minor assistance and guidance to be aware of all the advantages they can have by using the DEFeND platform. For instance, those requirements could be fulfilled by developing in the platform a social, collaborative forum, based on a social community, where the users can share their experiences, describe the advantages in using the platform to the other users, suggest to use functions of the platform, to give and receive suggestions, guidance, help and support using the platform. Therefore, on the basis of the citizen characterization, these solutions can fulfill user needs by increasing the system awareness of the users in relation to the usage of the DEFeND platform, to foster interaction, collaboration and in general a social behaviour that can provide a form of reciprocal assistance. Some indicative acceptance requirements are presented in Table 3

Table 3 should be placed here

6 Consolidating Requirements (Secondary Process)

In this paper we propose a holistic approach to collect software requirements that aim to address distinct user needs (i.e., functional, non-functional, legal, security, acceptance). Although this approach can assist software engineers to capture multiple aspects of the platform, it can also lead to a set of requirements that incorporate several repetitions and overlays. Therefore, we also introduce the necessity for a secondary processing of the resulting requirements, entitled *consolidation process*. In this section we demonstrate the steps comprised in the consolidation process and its application in the GDPR platform. The consolidation process that we propose includes six activities, described below:

1) Refinement of integrated requirements in terms of expression and clarity
2) Identification of commonalities, overlays and repetitions
3) Identification of functional groups
4) Prioritization of requirements
5) Legal review and refinement of requirements
6) Identification of out-of-scope requirements

6.1 Application of the Proposed Consolidation Process

The primary process of translating user needs into requirements resulted in 393 requirements in total, as depicted in Table 4.

Table 4 should be placed here

Although the overall elicitation process was conducted aiming at consistency, it still involved multiple software engineers and multiple perspectives; thus, the resulting requirements displayed a high degree of expression inconsistency, repetitions and overlays. Next, we demonstrate the application of the consolidation process in the collected software requirements.

6.1.1 Refinement of integrated requirements in terms of expression and clarity

In this activity we processed the 393 requirements in terms of wording, clarity and expression improvements. This step ensured that the requirements are clear to all readers and consistent terms and language is used across all requirements. As an example, different requirements included the terms “data processing agreements with third parties”, “data processing contracts with third parties”, “negotiation agreements with third parties”. This is because the end users might utilize different expressions to describe the same functionality, which is incorporated in the derived requirements. To ensure consistency we selected one term; i.e., in this case “data processing agreements with third parties”.

6.1.2 Identification of commonalities, overlays and repetitions

In order to identify commonalities, overlays and repetitions, all requirements were read through as a single document by individual readers. For triangulation purposes this process was conducted by four individual readers whose task was to read across all requirements and identify commonalities, overlays and repetitions. All findings were discussed until reaching consensus on the expression of the specific requirements.

6.1.3 Identification of functional groups

By processing the list of aggregated requirements, we inductively identified the presence of thirteen (13) groups of requirements:

1. Development of a GDPR privacy plan (33 requirements)
2. Creating a third-party management program (24 requirements)
3. Managing privacy complaints and individual rights (30 requirements)
4. Managing privacy incidents and breach notification (8 requirements)
5. Implementing Privacy by Design / Privacy Engineering (10 requirements)
6. Data de-identification/anonymization (3 requirements)
7. Meeting regulatory reporting requirements (15 requirements)
8. Addressing international data transfers (2 requirements)
9. Creating data Inventory and maps (26 requirements)
10. Conducting privacy risk assessments (PIAs/DPIAs) (12 requirements)
11. Obtaining and managing user consent (12 requirements)
12. Selection of appropriate security technical and organisational measures (6 requirements)
13. General platform requirements (77 requirements)

Each one of these groups comprised a set of requirements, which described the needs and expectations of the stakeholders from the platform with regards to a theme of functionalities. For example, the group ”Development of a GDPR privacy plan” includes several functionalities associated with the way that the platform should support an organisation to conduct self-assessment of GDPR readiness, to generate and monitor an action plan, to create reports that demonstrate compliance, and so on.

6.1.4 Prioritization of requirements

The previous consolidation activities reduced the requirements to 307. This list of requirements was processed in terms of priority, using the MoSCoW classification (Must have; Should have; Could have; Won't have). The team that applied the prioritization process considered the values attributed by the stakeholders during the requirements elicitation process. The stakeholder values were attributed in a scale of 0 to 5, therefore these values were homogeneously distributed into four ranges and each range was associated to a MoSCoW classifier, as described below:

- **Value Range 3.76 - 5 [MOSCOW Classification] Must have** -> Time-Critical, Important, Highest Impact above all in the short-term period, if not implemented the project is a failure
- **Value Range 2.6 - 3.75 [MOSCOW Classification] Should have** -> Not Time-Critical, Important, High Impact
- **Value Range 1.26 - 2.5 [MOSCOW Classification] Could have** -> Not Time-Critical, Not Very Important, Lower Impact, implemented if resources and time are in line with the plan, budget and timing
- **Value Range 0 - 1.25 [MOSCOW Classification] Won't have (this time)** Not Critical, Not Important or not appropriate at the moment, Very Low Impact, implemented it resources and time are in line with the plan, budget and timing

Besides the user value that was of primarily importance, there were also other parameters that were considered. In particular:

- When a requirement was derived from at least one legal requirement, the team opted for "Must";
- when a requirement was derived from at least one security requirement, the team opted for "Must";
- if a requirement was not derived from any legal or security requirements, the team considered the other requirements for checking if there were user values indications for deciding the prioritization for such requirement; specifically:
    - the team went through all the requirements indicated and, for each of them, the team reported the value associated; there the team reported either:
        - the direct value or not applicable (meaning that for the related question it was not asked to the user to provide a value in a range), if it was just one response,
        - or the average value, if more than one values have been indicated for the requirement
- the team calculated the average of the values for all the requirements indicated and, after converting the result in the MoSCoW value (according to the ranges indicated in the very first point of this list), the team reported for each requirement the MoSCoW classification followed by the value in parentheses, for instance “Must (4.0)”.

6.1.5 Legal Review and Refinement of Requirements

Given that the consolidation activities led to changing the wording of several requirements, a legal review of the requirements’ list was conducted to ensure that the final list of requirements are consistent with GDPR needs. This review process provided 33 critical comments, 26 comments of moderate importance and 7 comments of low importance. All comments were processed from a legal and technical point of view during workshops. All comments were addressed in ways that reflected an agreement between the legal and technical aspects. An example is provided in Table 5 below.

6.1.6 Identification of out of scope requirements

In the case that the software is developed for a pre-determined scope (i.e., as in the case of the DEFeND platform), a final activity is proposed for the identification of out of scope requirements (OOS). This is because the requirements were collected via open-ended questions, and thus the stakeholders may express needs that, although relevant to GDPR compliance, might not be within the scope of the respective project. Some criteria that were deemed relevant in the case of DEFeND include:

- **OOS 1: The scope of the DEFeND project is the organisation, it's not included third parties or joined controller.**
  - **Example:** Fun.REQ04.28 - The DEFeND platform shall provide a mechanism to view all third parties processing personal data on the company's behalf and view any associated submitted GDPR compliance self-assessment report.
- **OOS 2: The DEFeND project doesn't include this aspect.**
  - **Example:** Fun.REQ02.18 - The DEFeND Platform shall have a register of all data subject rights requests made by data subjects, showing the activities carried out (e.g. evaluation, approval, information request to data subject, etc.) and their respective status.
- **OOS 3: The pilots' scenarios don't include this option**.
  - **Example:** Fun.REQ10.06 - The DEFeND platform shall notify a processor about the instruction of the controller to stop processing certain personal data.
- **OOS 4: It's covered by another standard tool**.
  - **Example**: Fun.REQ04.44 - The DEFeND platform shall provide a list of Threats, ordered according to user-selected criteria.
- **OOS 5: The DEFeND Platform doesn't include integration with internal system**.
  - **Example**: Fun.REQ01.09 - The DEFeND platform shall allow to monitor data retention periods (especially in shadow IT).

We considered as 'out of scope' six requirements under the category OOS 1, nine requirements under the category OOS 2, three requirements under the category OOS 3, six requirements under the category OOS 4, nine requirements under the category OOS 5, and one requirement under more than one category.

6.2 Summary

In this section we proposed a consolidation process, as a final stage in the requirements elicitation process. We proposed at least six stages for the consolidation process. The list of derived requirements for the DEFeND platform included 393 requirements. The application of the consolidation process resulted in 307 requirements (after activities 1-4) and a final set of 273 requirements, after excluding OOS requirements.

7 Requirements' Engineering for a GDPR Compliance Platform: Lessons Learned

In this section we present the requirements engineering challenges that the consortium faced, the innovations that were applied, and the lessons learned from the process of eliciting and consolidating requirements for a GDPR compliance platform (Piras et al., 2019).

7.1 Academic Implications

During the preparation and validation of the data collection questionnaire we received significant feedback by DPOs working in the financial sector, as well as DPOs working within the organizations participating in the consortium; where two trends emerged. One trend was that the questionnaire was not adequate to capture completely all the needs. DPOs commented that questions should allow for open text as much as possible in order to allow relevant stakeholders to express their needs. In addition, interviews were highlighted as of paramount importance, which would need to include follow up questions. This feedback reveals the complexity of capturing requirements for a GDPR compliance platform. A second trend was that the questionnaire would require a lot of time to be completed by a participant and therefore should include only multiple-choice questions. This request can be explained by the DPOs' busy schedule and lack of time to complete the questionnaire. Therefore, a hybrid approach was followed which included interviews and a multiple-choice questionnaire. Interviews would be selected only when the GDPR compliance representative could afford to dedicate significant effort and time, while multiple choice questionnaire would allow receiving information from multiple stakeholders even if they did not have lots of time to devote.

Conducting effective requirements elicitation interviews is challenging. Some of the consortium partners were novice interviewers. Empirical evidence has shown that the methodological soundness and correct conduct of interviews is important (Davis et al, 2006). Therefore, to overcome this challenge a detailed interview protocol was developed and followed during the interviews. The interview questions were designed to allow the participants to openly express their expert opinion and needs on a subject matter. In several cases, the response of the participant triggered a new question or a more in-depth question. In these cases, we used the technique of mirroring (Myers & Newman, 2007), according to which the interviewer uses the interviewees' words and phrases to construct subsequent questions. This proved to be very successful as it established a common understanding and reduced the use of leading questions.

The needs of the citizens from a GDPR compliance platform were collected using an instructed questionnaire completion technique. In order to receive as detailed as possible responses, citizens were instructed to complete the questionnaire in the context of an online service that they are using from the four sectors that the project is interested in. This resulted in the collection of more meaningful responses and justified explanations by the citizens.

In contrast with the DPOs', citizens contributed a lot less in open-ended questions, this was expected due to the wide audience that the consortium sent the questionnaire to, and the challenges a citizen faces in fully understanding GDPR in this early stage that the regulation is enforced. Nevertheless, they highly expressed towards a platform that (i) enables them to clearly verify whether the basic GDPR principles and their rights are complied with when their data is processed by third parties, (ii) is user friendly and (ii) enables them to define their consent.

Besides the challenges in the elicitation of requirements there were also challenges in their consolidation. Without refining the elicited requirements in terms of expression and clarity, and in terms of commonalities and repetitions, it would have been overly laborious to manage the requirements throughout the DEFeND platform development lifecycle. Such a refinement resulted in requirements that are expressed in a form that is readable and traceable by everyone involved in the development, in order to manage their evolution over time. Establishing requirements traceability in the requirements documentation facilitates the management of changes in the requirements by being able to investigate the consequences and the impact of such changes.

Last, but not least, is the complication of requirements prioritization, which is burdensome because of social reasons. Reaching an agreement among different stakeholders that have divergent, or even conflicting goals is difficult. The approach followed was a win-win approach, which allowed the most vital goals to be met. Requirements that had been given a criticality value greater than '3.76' by the stakeholders were classified as 'Must' requirements and therefore must be implemented during the project. To this end, the most crucial goals of the stakeholders were identified and it was ensured that these goals will be met.

7.2 Industrial Implications

It is a widespread opinion that the implementation of the GDPR had led the financial sector to improve tools and methods for managing personal information in an optimized way, also increasing the awareness on the major repercussions on business processes and IT architectures. In other words, from a certain point of view the recent regulatory developments may be viewed as an opportunity for banks, raising the attention in establishing good practices in various data management areas. With this in mind, many banks have been working rapidly over recent years in improving incident monitoring, governing security and managing IT risks. This means that in the last years, the banks had implemented several tools and procedures to ensure compliance with the GDPR.

In this context, the value of a unique platform like DEFeND (Piras et al., 2019) could be in the possibility of supporting a continuous GDPR Maturity Assessment, in order to identify the most critical areas of compliance, plan the improvement actions and convey specific reports to different actors, also considering the existing standard and the evolution of best practices. However, our requirements elicitation process revealed that to leverage those opportunities, it is important that the GDPR platform represents a sort of orchestration engine, able to enforce a presidium on the different

data protection processes and able to seamlessly integrate with all the other systems and procedures that the bank has already put in place. To this extent, the possibility to have a modular solution is paramount (Piras et al., 2019).

7.3 Societal Implications

Europe, with GDPR, is leading the effort for the fundamental rights of data protection where citizens control their own data and can share it knowing their rights are being protected. However, such effort will only succeed if appropriate technological privacy solutions are put in place to support the implementation of GDPR and support its enforcement. The DEFeND platform is being implemented at pilot domains which are privacy sensitive and fundamentally linked to the wellbeing, prosperity and security of EU citizens (i.e., health care, banking, energy and public administration). Thus, the platform is expected to create significant impact towards data protection and could help restore citizen's confidence in the ability of those data controllers to maintain privacy of their data. Overall, DEFeND is expected to increase the privacy feeling of EU citizens, especially in terms of the usage of their private data for services that relate to the four domains. In the future, the DEFeND platform is expected to be used across Europe and across different domains to increase privacy of European citizens' personal data and empower them to actively engage in their management. The work conducted in this article aims to ensure that the DEFeND platform will integrate state of the art privacy solutions that can provide organizations and citizens with capabilities to understand and analyze personal data protection and identify adequate solutions to ensure the protection of personal data.

8 Conclusions

In this paper, we presented the methodology and process that was followed in a European project, DEFeND, in order to elicit, analyze and consolidate requirements for a GDPR compliance platform. This article extended earlier work (authors names removed for review), which, to the best of our knowledge, was the first paper to propose a software requirements elicitation methodology and process for GDPR compliance platforms. Following the primary data analysis to extract software requirements per distinct need (e.g., functional, legal) in this extended paper we describe the secondary analysis methodology and process through which we achieved the consolidation of the various requirements into a consistent set of platform software requirements.

The complexity of the process of software requirements' elicitation was challenging as it included the involvement of stakeholders from four different sectors, banking; energy; health; and public administration. The process was composed of several requirements engineering activities that were adapted in order to specify the requirements for a GDPR compliance platform including legal and privacy requirements, functional requirements, as well as acceptance requirements, for assuring that the users of the platform will embrace and use it. By offering a detailed description of the process followed we envision that we assist future software requirements academics and practitioners who may find this knowledge beneficial when developing similar GDPR software solutions. Further, through a software elicitation process that integrates various perspectives (i.e., security, legal, technology acceptance) we aim to develop a GDPR platform that can contribute to the established societal goals of the European Union, such as the European Digital Agenda and the Europe 2020 Strategy.

Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787068.

References

Bednar, K., Spiekermann, S., & Langheinrich, M. (2019). Engineering Privacy by Design: Are engineers ready to live up to the challenge?. The Information Society, 35(3), 122-142.

Bisztray, T., & Gruschka, N. (2019). Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality. In Nordic Conference on Secure IT Systems (pp. 3-19). Springer, Cham.

Blank, S.G. (2007). Four Steps to the Epiphany: Successful Strategies for Products that Win, Palo

Bryman A. (2008). Social Research Methods, 3rd Edition, Oxford University Press: Oxford; 2008.

Cavoukian, A. (2011). Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices. Available online at: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

Davis, A., Dieste, O., Hickey, A., Juristo, N., & Moreno, A. M. (2006). Effectiveness of requirements elicitation techniques: Empirical results derived from a systematic

review. In 14th IEEE International Requirements Engineering Conference (RE'06) (pp. 179-188). IEEE.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Re-quirements Engineering, 16(1), 3-32

European Data Protection Board (2019). First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities, Available online at: https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

Faßbender, S., Heisel, M., & Meis, R. (2014). Problem-based security requirements elicitation and refinement with pressure. In International Conference on Software Technologies (pp. 311-330). Springer, Cham.

Gartner (2017). Forecast Analysis: Information Security, Worldwide, 1Q17 Update., August 2017. Available at: https://www.gartner.com/en/documents/3889055

Gena, C. (2005). Methods and techniques for the evaluation of user-adaptive systems. The knowledge engineering review, 20(1), 1-37.

Horák, M., Stupka, V., & Husák, M. (2019, August). GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8).

IAPP (2018). 2018 Privacy Tech Vendor Report v.2.4e. Available online at: https://iapp.org/resources/article/2018-privacy-tech-vendor-report/.

ISACA (2019), GDPR The End of the Beginning, http://www.isaca.org/Knowledge-Center/Documents/2018-GDPR-Readiness-Survey-Report.pdf.

Juristo, N., Moreno,A. M., Dieste, O., Davis A. and Hickey, A. (2006). Effectiveness of Requirements Elicitation Techniques: Empirical Results Derived from a Systematic Review. In: 14th IEEE International Requirements Engineering Conference (RE'06)(RE), Minneapolis/St. Paul, Minnesota, USA, 2006, pp. 179-188.

Kalloniatis, C., Belsis, P., & Gritzalis, S. (2011). A soft computing approach for privacy requirements engineering: The PriS framework. Applied Soft Computing, 11(7), 4341-4348.

Kurtz, C., & Semmann, M. (2018). Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors.

Li, H., Yu, L. & He, W. (2019). The Impact of GDPR on Global Technology Development, Journal of Global Information Technology Management, 22:1, 1-6

Maguire, M. (2001). Methods to support human-centred design. International journal of human-computer studies, 55(4), 587-634.

Martin, Y. S., & Kung, A. (2018). Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 108-111). IEEE.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. ISJLP, 4, 543.

Mouratidis, H., & Giorgini, P. (2007). Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering, 17(02), 285-309)

Myers, M.D. & Newman, M. (2007). The Qualitative Interview in IS Research: Examining the Craft, Information and Organization (17:1), pp. 2-26

Notario, N., Crespo, A., Martín, Y. S., Del Alamo, J. M., Le Métayer, D., Antignac, T., ... & Wright, D. (2015, May). PRIPARE: integrating privacy best practices into a privacy engineering methodology. In 2015 IEEE Security and Privacy Workshop (pp. 151-158). IEEE.

Pavlidis, M., Islam, S., & Mouratidis, H. (2012). A CASE tool to support automated modelling and analysis of security requirements, based on Secure Tropos. In International Conference on Advanced Information Systems Engineering (pp. 95-109). Springer, Berlin, Heidelberg.

Pavlidis, M., & Islam, S. (2011). SecTro: A CASE Tool for Modelling Security in Requirements Engineering using Secure Tropos. In CAiSE Forum (pp. 89-96).

Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J. B., Fiorani, M., Magkos, E., Castillo Sanz, A., Pavlidis, M., D'Addario, R. and Zorzino, G. G. (2019). DEFeND Architecture: a Privacy by Design Platform for GDPR Compliance. In 16th International Conference on Trust, Privacy and Security in Digital Business-TrustBus, Springer, Linz (Austria), 2019.

Piras, L. (2018). Agon: a Gamification-Based Framework for Acceptance Requirements. Ph.D. dissertation, University of Trento, 2018.

Piras, L., Dellagiacoma, D., Perini, A., Susi, A., Giorgini, P. and Mylopoulos, J. (2019). "Design Thinking and Acceptance Requirements for Designing Gamified Software". In: 13th IEEE International Conference on Research Challenges in Information Science (RCIS), IEEE, Bruxelles (BE), 2019.

Piras, L. Paja, E., Cuel, R., Ponte, D., Giorgini, P. and Mylopoulos, J. (2017). Gamification Solutions for Software Acceptance: A Comparative Study of Requirements Engineering and Organizational Behavior Techniques. In: 11th IEEE International Conference on Research Challenges in Information Science (RCIS), IEEE, Brighton (UK), 2017.

Piras, L., Giorgini, P. and Mylopoulos, J. (2016). Acceptance Requirements and their Gamification Solutions. In: 24th IEEE International Requirements Engineering Conference (RE), IEEE, Beijing, 2016.

Piras, L. Paja, E., Giorgini, P. and Mylopoulos, J. (2017). Goal Models for Acceptance Requirements Analysis and Gamification Design. In: 36th International Conference on Conceptual Modeling (ER), Springer, Valencia (Spain), 2017b.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of Cybersecurity, 4(1).

Priyadharshini, G., & Shyamala, K. (2018). Strategy and Solution to comply with GDPR: Guideline to comply major articles and save penalty from non-compliance. In 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 190-195, IEEE.

Pulse Survey (2017). GDPR budgets top $10 million for 40% of surveyed companies. October 2017. Available online at: https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html

Thomson Reuters (2019). Study finds organizations are not ready for GDPR compliance issues, Available online at (accessed 5th April 2019): https://legal.thomsonreuters.com/en/insights/articles/study-finds-organizations-not-ready-gdpr-compliance-issues.

TrustArc (2018). GDPR Compliance Status. A comparison of US, UK and EU Companies. July 2018.

Tsohou, A., & Kosta, E. (2017). Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. Computer Law & Security Review, 33(4), 434-457.

Tsohou A., Magkos M., Mouratidis H., Chrysoloras G., Piras L., Pavlidis M., Debussche J., Rotoloni M. and Gallego-Nicasio Crespo B., (2019) Privacy, Security, Legal and Technology Acceptance Requirements for a GDPR Compliance Platform, 3rd International Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2019), Luxemburg, September 2019

Vanezi, E., Kouzapas, D., Kapitsaki, G. M., Costi, T., Yeratziotis, A., Mettouris, C., ... & Papadopoulos, G. A. (2019, May). GDPR Compliance in the Design of the INFORM e-Learning Platform: a Case Study. In 2019 13th International Conference on Research Challenges in Information Science (RCIS) (pp. 1-12). IEEE.

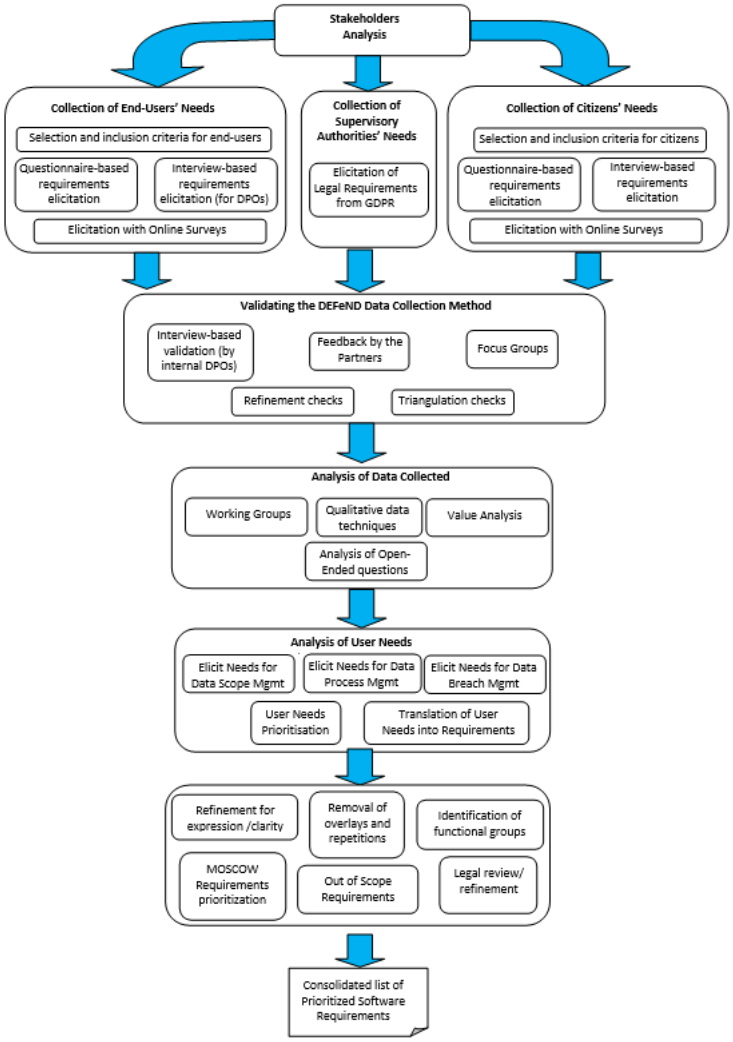

Figure 1: Methodological approach for eliciting software requirements for DEFeND Platform

Fun.REQ04	**Area: Data Scope Management**
Fun.REQ04.01	The DEFeND platform shall assess the GDPR compliance readiness of the organization based on the GDPR self-assessment.
Fun.REQ04.10	The DEFeND platform shall support the activity of DPIA.
Sec.REQ01	**Correct control and management of access to the system**
Sec.REQ01.02	The DEFeND platform should include an authorization mechanism based on need-to-know profiling.
Sec.REQ01.04	The DEFeND platform should include least privilege principle.

Table 1: Indicative functional and security requirements

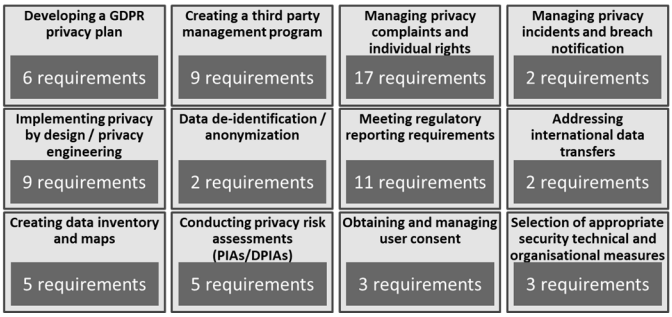

Figure 2: Distribution of Legal Requirements

Table 2: Indicative legal requirements

Leg.REQ01	**Developing a GDPR privacy plan**	**GDPR reference**
Leg.REQ01.04	The DEFeND Platform should provide tools to enable an organisation to draw reports in order to demonstrate compliance with its GDPR obligations and to compose the organisation's accountability file.	Art. 5(2), 24(1)
Leg.REQ02	**Creating a third party management program**	**GDPR reference**
Leg.REQ02.01	The DEFeND Platform should allow an organisation, when acting as a controller, to identify and map its relationships with processors.	Art. 28
Leg.REQ02.06	The DEFeND Platform should provide tools to assist an organisation, acting as controller, to keep track of data processing agreements.	Art. 28(3)

Table 3: Indicative acceptance requirements

NFun.REQ01	Acceptance Requirements
NFun.REQ01.03	The DEFeND platform shall offer a wide user acceptance and appreciation about it's features.
NFun.REQ06.02	The DEFeND platform shall make the citizen to perceive that the platform is useful in terms of the effectiveness of enabling her in managing her personal data and in having her rights fulfilled.
NFun.REQ06.04	The DEFeND platform shall make the citizen aware that the platform is promoted largely at the social level, for instance by important institutions and by the promoters of the platform

Table 4: Unconsolidated platform requirements

Category of requirements	**Number of requirements**
GDPR platform privacy and security legal requirements	74
GDPR platform technical security requirements	25
GDPR platform functional requirements	257
GDPR platform non-functional requirements	37
Total Requirements	**393**

Table 5: Indicative example of refinement of requirement following legal and technical review

Original requirement	**Fun.REQ04.53** The DEFeND platform shall support the enforcement of technical audit compliance readiness acceptance status as pre-requisite for third-party processor data-sharing contracts **Leg.REQ02.04** The DEFeND Platform should allow an organisation, acting as a controller, to assess whether its (intended) processors provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.
Consolidated requirement	The DEFeND platform shall support the enforcement of technical audit compliance readiness acceptance status as pre-requisite for third-party processor data-sharing contracts.
Legal and Technical Review comments on the Consolidated requirement	The wording of Leg.REQ02.04 and art. 28(1) GDPR should be well reflected in the requirement (Legal Review). The requirement should express a functionality that it will be possible to test if the produced software satisfies the requirement (Technical Review).
Final requirement	The requirement was rephrased as "The DEFeND platform shall support an organisation, acting as a controller, to assess and audit through a predefined questionnaire/ checklist its (intended) processors' compliance readiness acceptance status and whether such processors provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject."