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

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

Aggeliki Tsohou[1], Manos Magkos[1], Haralambos Mouratidis[2], George Chrysoloras[3], Luca Piras[2], Michalis Pavlidis[2], Julien Debussche[4], Marco Rotoloni[5] and Beatriz Gallego-Nicasio Crespo[6]

[1]Ionian University, Corfu, Greece
[2]University of Brighton, Brighton, United Kingdom
[3]University of the Aegean, Samos, Greece
[4]Bird & Bird, Brussels, Belgium
[5]ABI Lab, Rome, Italy
[6]Atos, Madrid, Spain

Abstract. GDPR entered into force in May 2018 for enhancing user data protection. Even though GDPR leads towards a radical change with many advantages for the data subjects it turned out to be a significant challenge. Organizations need to make long and complex changes for the personal data processing activities to become GDPR compliant. Citizens as data subjects are empowered with new rights, which however they need to become aware of and understand. Finally, the role of data protection authorities changes as well as their expectations from organizations. 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. To succeed, the platform needs to satisfy legal and privacy requirements, be effective in supporting organizations in GDPR compliance, 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 process, within the DEFeND EU Project, for eliciting and analyzing requirements for such a complex platform, by involving stakeholders from the banking, energy, health and public administration sectors, and using advanced frameworks for privacy requirements and acceptance requirements. The paper also contributes by providing elicited privacy and acceptance requirements concerning a holistic platform for supporting GDPR compliance.

Keywords: GDPR, compliance, software requirements, prioritisation.

1 Introduction

Since May 2018 the General Data Protection Regulation (GDPR) has become the center of attention for practitioners, researchers, States, 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 (Innovation Action) that is dedicated into delivering such a platform. 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 present the software engineering methodology and results that were followed to capture the needs of users and model 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. In this paper however we will emphasize on the financial sector and the respective lessons learned.

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 and Section 6 provides the knowledge that was learnt from this process and could be informative for similar endeavors. Finally, Section 7 concludes the paper.

2 The Defend Project and its Position in the Industry

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 built around 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). 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. PbD principles have not yet gained adoption in the engineering practice, mainly because a mismatch between the legal and technological mindsets (Martin & Kung, 2018) 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.

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).

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. At operational level, the platform, based on the PDC, will monitor and enforce data subject's preferences, and will notify users if any inconsistency will be identified.

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 27005:2011do 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).

The DEFeND project 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 based on international standard. This analysis will be

performed in an easy and user-friendly interface and it will not need a specific knowledge and expertise in security and/or risk analysis to be performed.

2.3 The DEFeND Project

The DEFeND Platform is an innovative data privacy governance platform, which will facilitate scoping and processing of data and data breach management and will support organisations towards GDPR compliance.

In order to comply with the GDPR, organisations have to implement in their processes, at a very low-level, different tools, solutions, and practices, as to inherently integrate privacy in these ones. Therefore, it is important that DEFeND will provide a solution that not only supports compliance of the relevant GDPR articles, but will also fulfill special characteristics of needs that organisations might have. DEFeND will go beyond current products that offer general solutions and need special expertise and effort in order to cover the requirements of the organizations.

DEFeND will be adaptable enough so that organisations with budget restrictions can still make use of it. We plan to achieve this by following a modular strategy providing different services to users and supporting both planning and operational stages. This allows two innovative aspects: on one hand the solutions will be more specific to the needs of the organization and, on the other hand, the modules of DEFeND could be extended with new solutions. The DEFeND platform will support not only organisations to comply with GDPR but also professional advisors (legal and/or technical).

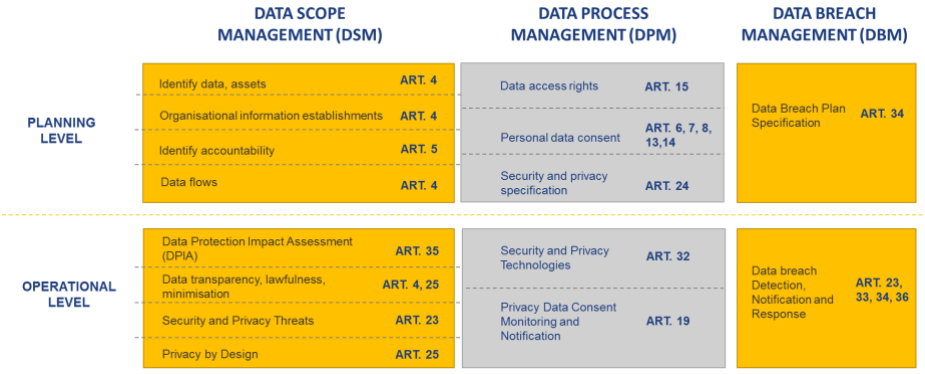

Fig.1: Three management areas of the DEFeND Platform

The project will achieve its aim by introducing a new paradigm, which we call Model-Driven Privacy Governance (MDPG). Such paradigm enables building (from an abstract to a concrete level) and analysing privacy related models following a Privacy-by-Design approach 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 as shown in Fig. 1.

More specifically, at the planning level, the platform will support the development of models of the organisational data that capture information required for GDPR compliance such as identification of data and assets (art. 4), Organisational Info and

establishments (art. 4), Data Transparency, Lawfulness and Minimisation (art. 25), personal data consent (art. 6,7,8,13,14) and data breach information (art. 34). Concretely, the DEFeND platform will support the transformation of planning models to operational models that are employed to perform analysis that supports Data minimisation, Data Protection, Impact Assessments (art. 35) and Privacy-by-Design and Privacy-by-Default principles (art. 25). At the operational level, the project will bring together security and privacy methodologies, encryption and anonymization tools and policy enforcers.

These management areas could be seen as the main services that the platform will provide to organizations and relevant stakeholders. Each one of these services assists organisations to collect, analyse and operationalise different aspects and articles of the GDPR and provide appropriate reporting capabilities.

To support those services, the platform consists of five (5) back-end components: Data Assessment Component, Data Privacy Analysis Component, Privacy Specification Component, Privacy Implementation and Monitoring Component, Data Breach Component. Each component includes a number of modules aiming to deliver functionalities (Fig. 2). The modules will be developed by enhancing software tools, services and frameworks of the project partners. Moreover, the platform includes a dashboard, which works as the main front-end between the platform and its users.

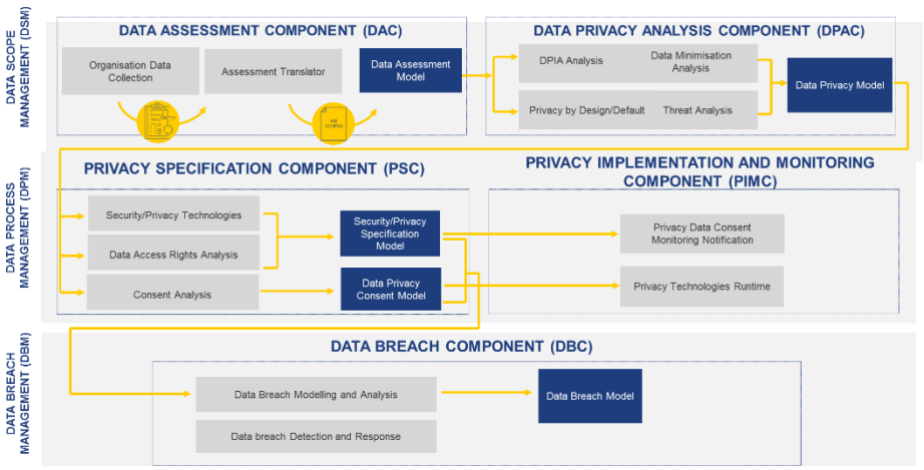

Fig.2: DEFeND Platform Modules

3 An 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.

There are different roles that could provide functional requirements, which would reflect different perspectives. It was considered as very crucial to cover a diverse cross-section of different stakeholders, so that the produced list of user needs and requirements are not skewed towards a particular direction. The most critical is the perspective of the roles regarding compliance and auditing (e.g., DPO). The consortium identified the possible users in different scenarios and classified them, according to their types:

1. *Internal Stakeholders:* Stakeholders who are responsible for activities regarding the GDPR compliance in an organization. Candidate roles were:
   - *a)* Data Protection Officer (DPOs)
   - *b)* Chief of the Organization
   - *c)* Chief Data Officer
   - *d)* IT manager/technician
   - *e)* Risk Assessment Officer
   - *f)* Audit Officer

   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.
2. *External Stakeholders:* External stakeholders included citizens as data subjects when interacting with industry providers:
   - *a)* Within the health sector
   - *b)* Within the banking sector
   - *c)* Within the public administration sector
   - *d)* Within the energy sector
3. *Supervisory (Data Protection) Authorities:*Supervisory authorities are considered as external stakeholders of the DEFeND platform. The functional requirements for the supervisory authorities are mostly described by GDPR itself.

3.2 Privacy and Security Needs

The DEFeND platform will support privacy-by-design development of new services and systems, to allow natural integration of security and privacy of data in organizations. To achieve that, the project is dedicated to the rigorous definition of pilot scenarios, user privacy and compliance requirements using a systematic approach for end-users and citizens' security/privacy and functional needs collection, analysis and translation in prioritized requirements, to be included in the platform.

Furthermore, the DEFeND project will use, as part of the Data Privacy Analysis Component (DPAC), state-of-the-art requirements engineering methodologies, 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) security-aware software systems development methodology and related tool (SecTro), which is used in the DEFeND project to elicit, model and analyse the privacy and security requirements of the platform, and which will also be 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.
The functional requirements of the platform will be identified, defined and formalized in terms of use case diagrams and SRS (software requirements specification) as established by related standards[1], while a priority will be associated which each requirement.

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 (e.g., Data Controllers, Data Processors, Data Subjects, IT technicians, lawyers, etc.). The

[1] IEEE Guide for Software Requirements Specifications, IEEE Std 830-1984.

platform must support functionalities that are appreciated, accepted and used by all types of users involved.

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. In particular, DEFeND partners identified the *key stakeholders*, and for each user category, a questionnaire was prepared, aiming at capturing the DEFeND 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, i.e., Data Scope Management (DSM), Data Process Management (DPM), and Data Breach management (DBM). The overall approach is depicted in Fig. 3.

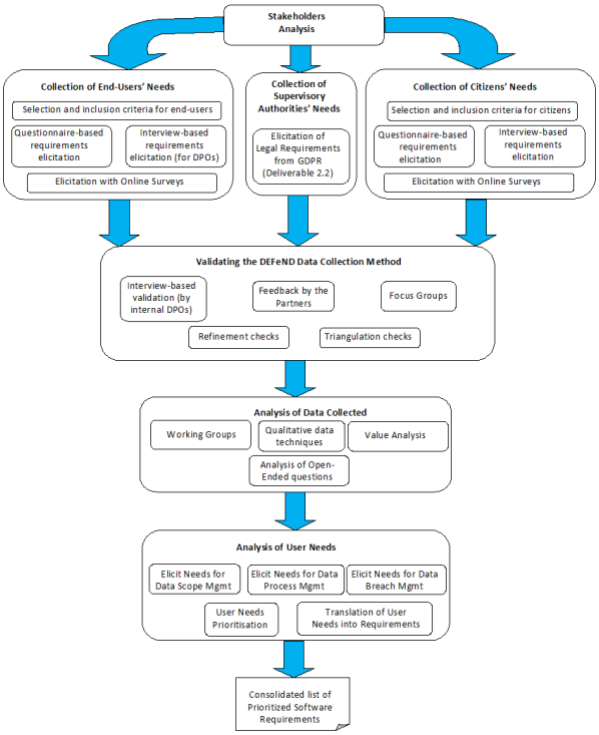

Fig.3: Methodological approach for eliciting software requirements for DEFeND Platform

4.1 Preparation of Questionnaires

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:

Customer Segmentation. A relevant action point was to consider the possibility of different questionnaire versions depending on the role of the participant in end-user organizations. In addition, each participant citizen completed the questionnaire having in mind only his/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[2] section regarding user information, questions 1-5 and background information, questions 6-15.

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

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

about new problems and challenges as conceived by the interviewees. This category is supported by questions 16-22.

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.

4.2 Validation of Questionnaires

The initially prepared questionnaire was commented by the Data Protection Officer (DPO) of each partner in the project consortium. The inputs received by all partners' DPOs have helped to significantly alter the initial questionnaire and/or the information collection process. All feedback was collected and processed by the technical partners.

One of the major requirements gathering objectives was to receive opinions or comments from members of a specific sector about the questionnaire. One partner of the project has sent the questionnaire to the banking sector stakeholders who would participate in a focus group during a subsequent partners meeting. Indeed, DPOs and IT managers from various organizations in the banking sector have participated either physically or via conference call. The session included an initial introduction by one partner of the project, a round table discussion with the participants and a final part with question and responses. The objective of this session was to gather feedback from this group of end-users on the questionnaire (with respect to structure, text of the questions, format of the questions/answers, language used, etc.) which was shared with them in advance. The result of this stage was a consolidated draft of the questionnaire for the end users.

4.3 Data Collection Approach

We collected data regarding the needs of the platform's users by participants from seven European countries (i.e., Italy, Greece, Spain, Bulgaria, France, Portugal, UK), spanning the two main user roles; organizations and citizens. The profile of participants for organizational needs, was described as an individual responsible for the coordination and monitoring of activities regarding the GDPR compliance. The profile of participants for citizens' needs was described as 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. Further, 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 the main expected user role for 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 guarantee the separation of duties to prevent fraud and error when processing personal data, and also 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. Other

features that were highlighted as mostly important was the ability of the tool to measure the privacy level that the organization achieves and to analyze and select the security measures for risk mitigation.

- At the Data Process Management area, the most important feature according to the end-users was to provide support for implementing security and privacy controls (e.g., anonymisation, encryption and authorisation).

At the Data Breach Management, end users pointed out the criticality of the real-time notification of the data subjects about privacy violations.

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 2.

Table 1: Indicative functional and security requirements

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.

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: Developing a GDPR privacy plan, Creating a third party management program, Implementing privacy by design / privacy engineering, Managing privacy complaints and individual rights, Data de-identification / anonymization, Creating data inventory and maps, Conducting privacy risk assessments (PIAs/DPIAs), Meeting regulatory reporting requirements, Obtaining and managing user consent, Managing privacy incidents and breach notification, Addressing international data transfers, and Selection of appropriate security technical and organisational measures.

Towards defining the privacy and security legal requirements necessary to be used as basis for building the DEFeND Platform, the project 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.

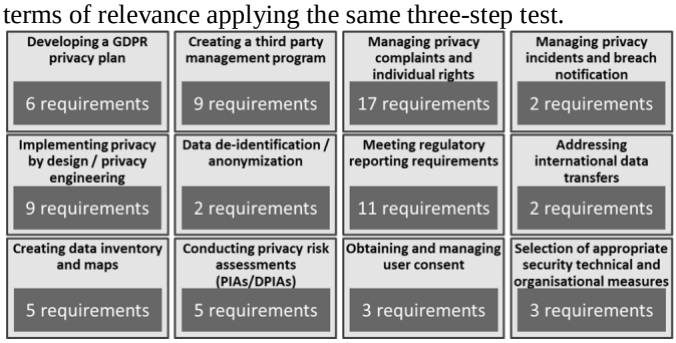

Fig.4: Distribution of Legal Requirements

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. 4.

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)

Some indicative legal requirements in the areas 'Developing a GDPR privacy plan' and 'Creating a third party management program' are presented below in Table 3.

5.3 Acceptance Requirements

The analysis of the questionnaire responses, in particular the questions targeting the elicitation of acceptance requirements, provided us with information to characterize the different users of the DEFeND platform.

Regarding the citizen role, we discovered that male citizens, young citizens, socializers who are not obliged to use the system, are more prone to accept the DEFeND platform. Further, we identified acceptance requirements which will assist in designing and enhancing the DEFeND platform architecture, in a way that it can really support and motivate all the stakeholders, by supporting usability, ease of use, awareness of the framework and guidance. Among the most important aspects pertaining the acceptance requirements is the need of users for social interaction and collaboration with other users. Such requirements provide insights into platform features, such as the integration of a social, collaborative forum to enable user communities, 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. Some indicative acceptance requirements are presented in Table 4.

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

6 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.

6.1 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.

6.2 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 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.

7 Conclusions

In this paper, we have presented the process that was followed to elicit and analyze requirements for a GPDR compliance platform. The complexity of the process was

high as it included the involvement of stakeholders from four different sectors, banking; energy; health; and public administration. The process is composed of several requirements engineering activities that were adapted in order to specify the requirements for a GDPR compliance platform including functional, non-functional, security, privacy, legal and acceptance requirements. Finally, the challenges and lessons learned from this process were summarized and presented.

Acknowledgments

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

References

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 re-quirements. 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.

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.

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.

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. (2018). 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), 2017.

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.