DEFeND architecture: a privacy by design platform for GDPR compliance.

PIRAS, L., AL-OBEIDALLAH, M.G., PRAITANO, A., TSOHOU, A., MOURATIDIS, H., GALLEGO-NICASIO CRESPO, B., BERNARD, J.B., FIORANI, M., MAGKOS, E., SANZ, A.C., PAVLIDIS, M., D'ADDARIO, R. and ZORZINO, G.G.

2019

DEFeND Architecture: a Privacy by Design Platform for GDPR Compliance

Luca Piras[1], Mohammed Ghazi Al-Obeidallah[1], Andrea Praitano[2,3], Aggeliki Tsohou[4], Haralambos Mouratidis[1], Beatriz Gallego-Nicasio Crespo[5], Jean Baptiste Bernard[6], Marco Fiorani[6], Emmanouil Magkos[4], Andrès Castillo Sanz[7], Michalis Pavlidis[1], Roberto D'Addario[2], and Giuseppe Giovanni Zorzino[2,3]

[1] Centre for Secure, Intelligent and Usable Systems,
University of Brighton, Brighton, United Kingdom
{l.piras,m.al-obeidallah2,h.mouratidis,m.pavlidis}@brighton.ac.uk
[2] Maticmind SpA, Rome, Italy
{andrea.praitano,roberto.daddario,bgiuseppe.zorzino}@maticmind.it
[3] UNIHermes, Rome, Italy
{andrea.praitano,bgiuseppe.zorzino}@unihermes.org
[4] Ionian University, Corfu, Greece
{atsohou,emagos}@ionio.gr
[5] Atos, Madrid, Spain
beatriz.gallego-nicasio@atos.net
[6] Gridpocket SAS, Valbonne Sophia Antipolis, France
{jean-baptiste.bernard,marco.fiorani}@gridpocket.com
[7] International University of La Rioja UNIR, Madrid, Spain
andres.castillo@unir.net

Abstract. The advent of the European General Data Protection Regulation (GDPR) imposes organizations to cope with radical changes concerning user data protection paradigms. GDPR, by promoting a Privacy by Design approach, obliges organizations to drastically change their methods regarding user data acquisition, management, processing, as well as data breaches monitoring, notification and preparation of prevention plans. This enforces data subjects (e.g., citizens, customers) rights by enabling them to have more information regarding usage of their data, and to take decisions (e.g., revoking usage permissions). Moreover, organizations are required to trace precisely their activities on user data, enabling authorities to monitor and sanction more easily. Indeed, since GDPR has been introduced, authorities have heavily sanctioned companies found as not GDPR compliant. GDPR is difficult to apply also for its length, complexity, covering many aspects, and not providing details concerning technical and organizational security measures to apply. This calls for tools and methods able to support organizations in achieving GDPR compliance. From the industry and the literature, there are many tools and prototypes fulfilling specific/isolated GDPR aspects, however there is not a comprehensive platform able to support organizations in being compliant regarding all GDPR requirements. In this paper, we propose the design of an architecture for such a platform, able to reuse and integrate peculiarities of those heterogeneous tools, and

to support organizations in achieving GDPR compliance. We describe the architecture, designed within the DEFeND EU project, and discuss challenges and preliminary benefits in applying it to the healthcare and energy domains.

Keywords: Privacy by Design · Privacy Engineering · Security Engineering · Data Protection · GDPR

1 Introduction

Information and Communication Technologies (ICT) playes a significant role in the every-day life. New technological advances such as Cloud Computing, Internet of Things and Big Data provide benefits and have changed the way we store, access and exchange information. The rapid development and advances in ICT have led to their adoption by organizations (enabling them to transform business to digital services, increasing efficiency), public authorities (enabling them to provide new services to citizens and to reduce complexity) and individuals (enabling them to communicate and share personal information faster and efficiently).

However, together with all the benefits that such technologies bring, opportunities (deliberate or accidental) for misuse of citizen data are also created mostly due to lack of control over management and privacy issues of citizen data. To react to such challenge, organizations have to adopt solutions that support with an end-to-end data protection governance, which can adapt to the specific characteristics of different sectors. To cover these regulatory gaps, and to force organizations to guarantee citizens rights, the European General Data Protection Regulation (GDPR) has been proposed. Even though GDPR aims to enforce and guarantee data subjects (e.g., citizens, customers) rights - for instance, enabling data subjects to be more aware regarding the usage of their data, and taking decisions over them (e.g., revoking usage permissions, asking for a fast data removal) -, it is important to note that it introduced also important challenges and difficulties for organizations, which led in many cases, since GDPR is in force, organizations to pay heavy fines for not being fully GDPR compliant [3].

Organizations are facing those problems for many reasons. Most of them are related to the nature of GDPR, which is a very long, complex regulation, covering many aspects, not providing details concerning technical and organizational privacy and security measures needed, and therefore it is difficult for organizations to be fully GDPR compliant. In fact, GDPR, by promoting a Privacy by Design and Privacy by Default approach, obliges organizations, in a not clear way, to change heavily their methods regarding the acquisition, management, processing of user data, as well as the monitoring of data breaches, notification, and definition of prevention plans for reducing the possibility that breaches happen, and to reduce also the potential damage. To be GDPR compliant, organizations are required also to trace precisely activities performed on user data, and are required to supply authorities with detailed information on this. Thus, authorities are enabled to monitor and to sanction more easily the organizations.

Therefore, organizations need tools and methods able to support and guide them in achieving full GDPR compliance [11]. This means, for instance, a support for: **(i)** analysing and understanding the current GDPR compliance level of an organization; **(ii)** selecting which GDPR aspects should be fulfilled by the organization (i.e. not all GDPR aspects should be satisfied by all the organizations; in fact it depends on the current situation, business and needs of the specific organization, and, thus, the challenge is to understand which subset of GDPR should be addressed); **(iii)** understanding which are the actions required to achieve GDPR compliance, preparing a plan for this, and having ready-to-use items and guidance for carrying out this complex process; **(iv)** providing the user with functionalities for exercising her rights; **(v)** being prepared to provide authorities with the documentation expected, and to interact with them.

Within a European project[1], we reviewed tools and prototypes from the industry and the literature, and found that there are many tools and prototypes able to fulfil specific/isolated GDPR aspects, however a comprehensive platform able to support organizations in being GDPR compliant in relation to all the GDPR requirements does not exist. In this work, we propose the design of an architecture for such a platform, able to reuse and integrate peculiarities of those heterogeneous tools, and to support organizations in achieving GDPR compliance. This paper presents an architectural solution to this challenge, which empower organizations to protect personal data according to GDPR, and that is applicable to heterogeneous sectors. Specifically, in this work, we describe the architecture that has been designed within a EU project, the Data govErnance For supportiNg gDpr (DEFeND)[1], and discuss challenges and preliminary benefits in the application of it to the healthcare and energy sectors.

The rest of the paper is organized as follows: Section 2 presents the conceptual idea around the DEFeND platform and the methodological and technical approach adopted. The architectural design and functionalities of the DEFeND platform are explained in Section 3. Section 4 presents multi sectors piloting of the platform, and Section 5 provides the related work, and compares it with the DEFeND solution. Finally, conclusions and future work are discussed in Section 6.

2 The Conceptual Foundations of the DEFeND Platform

We start illustrating conceptual aspects and challenges of the DEFeND platform. Then, we describe our methodological and technical approach for tackling this.

2.1 The DEFeND Concept and Challenges

DEFeND[1] is an Innovation Action project focusing on improving existing software tools and frameworks, designing and developing new integration software, driven by market needs, to deliver a unique organizational data privacy governance platform, for facilitating data scoping, processing, data breach management, by a

[1] DEFeND is a EU H2020 project: `https://www.defendproject.eu/`

privacy by design approach, and supporting organizations for GDPR compliance. To comply with GDPR, organizations have to implement in their processes different tools, solutions, and practices, as to inherently integrate privacy in those ones. Thus, it is fundamental for the DEFeND platform to provide a solution that not only supports compliance of the relevant GDPR articles, with a privacy by design approach, but also that fulfils specific organizations' needs.

GDPR considers many different aspects, and calls for the collaboration of heterogeneous professionals, with different skills and responsibilities in the organization. Professionals receive GDPR compliance support by different tools, each one covering only a small subset of GDPR aspects. Thus, the main challenge for the DEFeND platform is to provide support for all the different aspects for achieving GDPR compliance, according to the specific requirements of an organization. Main goals of DEFeND are to have: **(i)** a comprehensive platform able to support the organization in whole GDPR compliance; **(ii)** a platform able to fit heterogeneous contexts and dimensions of organizations; **(iii)** a modular, extensible platform that the organization can extend through tools and solutions based on its needs.

2.2 Methodological and Technical Approach

The DEFeND Platform is based on a novel technical approach we call Data Privacy Governance for Supporting GDPR (DEFeND)[1]. To support the modular approach and the GDPR compliance, we designed the platform architecture with a series of software components based on solutions that focus on each of the areas of GDPR [1] (e.g. conceptual languages to support privacy-by-design [11] or automated tools to support consent management). The DEFeND platform works as an orchestrator of the functionalities provided by the different components. We follow a Model-Driven Privacy Governance (MDPG) technical approach that enables building and analysing, from an abstract to a concrete level, privacy related models by 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. The DEFeND

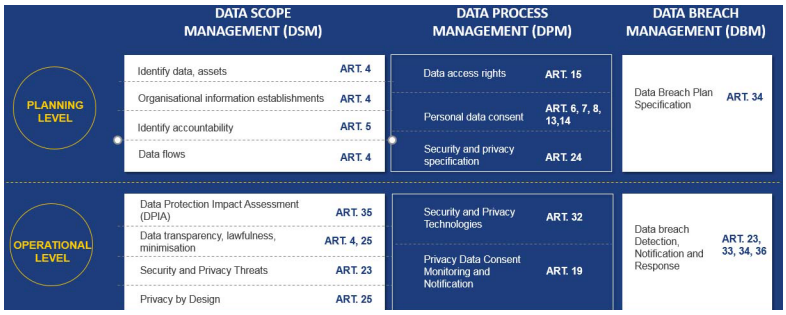

Fig. 1. Three management areas and two operational levels of DEFeND Platform

platform at the planning level (Fig. 1) focuses on supporting the development of models of the Organizational Data, which capture information required for

GDPR compliance such as identification of Data and Assets, Organizational Info and Establishments, Data Transparency, Lawfulness and Minimization, Personal Data Consent and Data Breach Information [3]. At the operational level, the platform supports the transformation of planning models to operational models, which are used to perform analysis for Data minimisation, Data Protection Impact Assessments, Privacy-by-Design and Privacy-by-Default principles [3]. The platform includes also functionalities to support GDPR reporting and notifications to data controllers/processors, consent and data breach notifications to Data Subjects, and GDPR Organizational Reporting to relevant authorities.

Moreover, we designed the DEFeND platform and architecture also on the basis of four procedural pillars: **(i)** *User Engagement* of heterogeneous kinds of stakeholders [14] (i.e. local public administration authorities, employees and citizens) from early stages of platform development, definition of functional and non-functional requirements (e.g., privacy, security, legal and acceptance requirements [14]), specification of realistic pilots and software validation; **(ii)** *Integration* of the various components through interconnected activities via implementation of appropriate interfaces and linkage mechanisms; **(iii)** *Piloting*, i.e. validation via real-life pilots in the healthcare, energy, banking, public administration sectors; **(iv)** *Training* via a program based on deep analyses of pilot organizations and their needs (e.g., software acceptance needs [14]), for creating awareness of privacy issues and privacy culture in the organization.

3 The Architecture of the DEFeND Platform

The architecture of the DEFeND Platform, shown in Fig. 2, is composed of 5 main services: *Data Scope Management Service, Data Process Management Service, Data Breach Management Service, GDPR Planning Service and GDPR Reporting Service*. Each one assists organizations to collect, analyse and operationalize

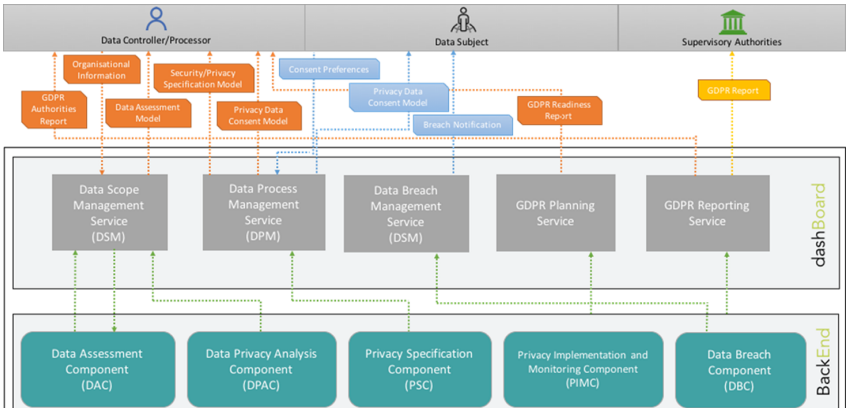

Fig. 2. The DEFeND Platform Architecture with Dashboard, Services and Components

different aspects and articles of GDPR [1], and provides appropriate reporting capabilities. To support those services, the platform consists of 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 modules that are the result of the extension of software tools, services and frameworks (described in the related work section), developed within national and international projects. The platform has a dashboard working as front-end among the platform and its users.

We designed the platform in a modular, flexible way, by following a Model-Driven Privacy Governance (MDPG) technical approach, and our novel DEFeND approach, we call Data Privacy Governance for Supporting GDPR (DEFeND[1], Section 2.2). Its modular, flexible architecture helps to increase the possibility to employ it in as many as possible heterogeneous domains, with different organizational needs. While, our DEFeND approach helped us in designing an architecture that, through its components, covers each areas of GDPR [1] (Fig. 2). Furthermore, its MDPG components support a privacy by design workflow, by employing conceptual languages and automated tools [11]. Moreover, thanks to our DEFeND and MDPG approaches, we designed architectural components supporting a privacy by design workflow able to guide, from abstract to concrete levels, the analysis of privacy related models spanning over 2 levels, the Planning Level and the Operational Level, and across 3 management areas, i.e. Data Scope, Data Process and Data Breach (Fig. 1, Fig. 2). The next subsections describe the architectural components, modules, interactions, workflow, and dashboard.

3.1 Data Assessment Component (DAC)

DAC (Fig. 3) supports the elicitation of organizational information and transforms them for the Data Analysis Privacy Component. DAC is based on next modules.
Organization Data Collection (ODC) Module. ODC, extending BE-Assess tool[2], provides an Organizational Data Questionnaire collecting information related to organizational scope, list of data processing, status of privacy processes and activities. It is used by the organization (data controller and data processor/s) to evaluate the status of the organization regarding parts relevant to GDPR. Moreover, ODC allows organizations to create a self-characterisation (e.g., size, available privacy/GDPR expertise) for recommending specific modules of the DEFeND Platform that the organization requires.
Assessment Translator (ATr) Module. ATr, extending BE-Assess tool[2], takes as input the Organizational Data Questionnaire from ODC, and translates it into an XML schema used to create the Data Assessment Model (DAM). DAM is a goal-based requirement engineering model of organizational data, including information concerning organization actors, assets, establishments and data flows.

3.2 Data Privacy Analysis Component (DPAC)

On the basis of DAM, DPAC performs Data Protection Impact Assessment, Data Minimisation analysis and Privacy-by-Design/Default and Threat analysis (Fig. 3). Analysis results are used for creating the Data Privacy Model. Such

[2] `https://www.maticmind.it/`

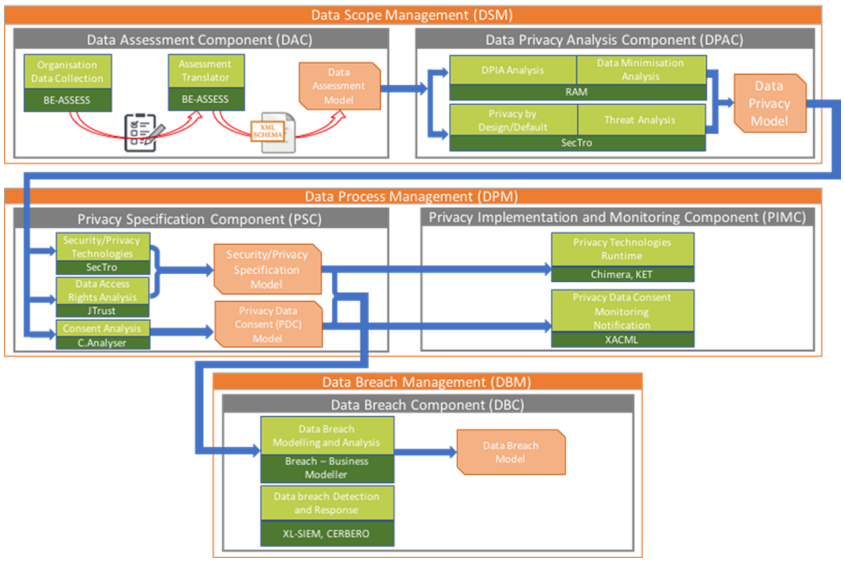

Fig. 3. Main components of the DEFeND Platform and their interactions

model provides a strategic conceptual model that clearly defines operational aspects of Data Scope Management and supports organizations to deal with GDPR [3]. DPAC can perform these activities on the basis of the RAM[2] and SecTro tools [11], and by extending them with the next modules.

DPIA Analysis (DPIA) Module. It is based on the RAM[2] tool. It enables organizations to measure and review their privacy level, and if necessary proposes design changes. Moreover, it includes safeguards privacy/security measures for mitigating potential risks. Its analysis results are used to create DPM.

Privacy-by-Design/Default (PbD) Module. This is based on the state-of-the-art goal-oriented security and privacy requirements engineering method Secure Tropos [11]. The method and its tool are extended to support the GDPR privacy by design/default requirement. PbD supports organizations in understanding security and privacy requirements, and design systems and services fulfilling those requirements. This forces organizations to deeply consider privacy since first phases of the software engineering process and not as an afterthought.

Data Minimisation Analysis (DMAn) Module. DMAn extends RAM[2] for supporting the analysis of data usage for ensuring the application of the data minimisation principle of GDPR, fostering organizations to process only personal data needed to achieve processing purposes.

Threat Analysis (ThAn) Module. This enables the modelling and analysis of privacy threats on personal data held by organizations. Threat analysis includes identification of relevant vulnerabilities, attack methods and potential malicious actors. ThAn, extending SecTro [11] and RAE[3] tools, supports threat assessment through combining different sources of information such as vulnerability scans and real-time monitoring of the infrastructure.

[3] `https://atos.net/en/`

3.3 Privacy Specification Component (PSC)

PSC processes DPM through the following modules.
Consent Analysis (CAn) Module. This takes the organizational privacy information included in DPM and data subject consent preferences from data subjects (requested through the DEFeND Platform dashboard). CAn extends CAnalyzer[4] and Privacy Level Agreements to support elicitation, analysis and specification of data subject consent and creates a Data Privacy Consent (DPC) Specification in the form of Data Privacy Consent Model (DPCM). DPCM is used by the Privacy Implementation and Monitoring Component (PIMC) to visualize, monitor and enforce data subject consent.
Data Access Rights Analysis (DARA) Module. DARA extends JTrust [11] and EPICA[3] tools supporting generation of policies for controlling data access, usage and information processing. It supports elicitation, modelling and analysis of data access rights scenarios by analysing potential access requests, how these are processed within the organization, and how information is provided to the data subject. Analysis results feed the Security/Privacy Specification Model.
Security/Privacy Technologies (STT) Module. This supports the selection of optimal security/privacy configurations with respect to criteria such as security/privacy requirements priorities and the severity of threats. Specifically, it extends SecTro [11] supporting expressions related to mitigation level of threats and goals of the systems (e.g., cost and performance) as cost-functions to be optimized. STT output feeds the Security/Privacy Specification Model.

3.4 Privacy Implementation and Monitoring Component (PIMC)

PIMC leverages the Privacy Data Consent Model and the Security/Privacy Specification Model for supporting run-time implementation of privacy technologies and monitoring, enforcement and notification of the Privacy Data Consent. PIMC has been designed with the next modules.
Privacy Technologies Runtime (PCR) Module. On the basis of models, obtained via PSC, this module guarantees the execution of the relevant security/privacy technologies across three main areas: encryption (extending KET[3]), authorisation (extending EPICA[3]) and anonymization (extending CHIMERA[5]). In terms of encryption, it supports key management and encryption of relevant sensitive data using a wide range of different encryption strategies to fulfil needs of as many as possible heterogeneous organizations. Regarding authorisation, it controls access based on the specification derived from the Data Access Rights Analysis, covering also location and time aspects. Concerning anonymization, PCR supports ingestion of data (structured and non-structured) and a high-level Domain Specific Language for data transformation and anonymization.
Privacy Data Consent Monitoring and Notification (PDCMN) Module. It is based on the XACML[3] and EPICA[3] tools, and includes a Privacy Data

[4] `https://www.visioneuproject.eu/`
[5] `https://www.pdmfc.com/`

Consent Monitoring enforcer and notifier. It supports organizations to enforce and monitor the Privacy Data Consent Model, by automatically filtering traffic and removing data that the data subject has not consented to share. Furthermore, if there is an attempt to share data without appropriate consent, PDCMN provides a notification to both data controllers and data subjects.

3.5 Data Breach Component (DBC)

DBC is responsible for modelling, analysing, detecting and responding to data breaches. On the basis of the Security/Privacy Specification Model and the Privacy Data Consent Model, provided by PSC, it enables organizations to develop, at planning stage, a data breach model, which is then used at run-time to detect, notify and respond to data breaches. It includes next modules (Fig. 3).
Data Breach Modelling and Analysis (DBMA) Module. By extending the Business Modeller tool [11], DBMA supports organizations to create the Data Breach Model. A model including a representation of the organization business processes, along with data flows and relevant security and privacy requirements. DBMA also supports analysis, on the model, for the definition of response plans to potential threats and data breaches.
Data Breach Detection and Response (DBD) Module. It is based on the XL-SIEM[6] and CERBERO[7] tools, for providing an information management system receiving input from various sources (both from the platform, for instance DBM, and from external sources such as threat identification websites), evaluating such information and detecting, notifying and responding to potential data breaches. DBD generates a data breach bulletin offering information concerning potential data breaches, and notifies organizations about data breaches.

3.6 Platform Dashboard

The platform dashboard (top of Fig. 2) acts as a front-end between users (Data Controllers/Processors, Data Subjects and Supervisory Authorities) and platform back-end components. On the one hand, it provides organizations with control over creation, deployment, and monitoring of data privacy governance strategies helping them to achieve GDPR compliance. On the other hand, it enables data subjects to use the platform offering consent related activities required by GDPR.

Specifically, the dashboard provides organizations with privacy related capabilities to: **(i)** *Input organizational Info into the platform*, supported by DAC through an easy to understand and interactive questionnaire; **(ii)** *Create, View and modify organizational Privacy related models*, concerning the Data Assessment Model, Data Privacy Model, Security/Privacy Specification Model, Privacy Data Consent Model, and Data Breach model; **(iii)** *Implement Privacy Technologies*, enabled through PIMC; **(iv)** *Monitor and Receive notifications about data*

[6] `https://atos.net/en/`
[7] `https://www.maticmind.it/`

subject consent and data breaches, supplied by PIMC and DBC; **(v)** *Monitor and evaluate GDPR compliance readiness*, supported by PIMC and DBC.

The dashboard provides data subjects with functionalities to: **(i)** *Define Consent Preferences*, allowed through the Consent Analyzer of PSC; the input is taken into account on the creation of the Data Privacy Consent model, which is used to monitor and enforce data subject consent management; **(ii)** *Receive Notification about Consent violations*, obtained through the Privacy Data Consent Monitoring and Notification module of PIMC; **(iii)** *Receive notifications about data breach*, offered through the Data Breach Component (DBC).

Finally, the dashboard includes specific GDPR supporting modules: **(i)** a *GDPR Planning Service* that supports the collection of information from the platform models, and its visualisation based on GDPR requirements; the result is a visual representation of the GDPR readiness of the organization and the ability to define a plan of action to achieve compliance; **(ii)** a *GDPR Reporting Service* that supports the collection of information required for GDPR reporting purposes; such information is encapsulated in the platform models, and can be visualised through the dashboard and shared with authorities.

4 Multi Sectors Piloting of the Platform

In the next 2 subsections, we discuss challenges and preliminary benefits in the application of the DEFeND platform to the healthcare and energy sectors.

4.1 Challenges and DEFeND Benefits in the Energy Sector

The recent and massive deployment of Smart Meters in many EU countries has raised many questions linked to privacy and data protection rights. Smart meters are a new generation of energy consumption readers, capable of connecting via digital networks, sending real time information back to energy grid consumption systems, and monitoring companies with a high temporal resolution rate [16]. The appearance of this technology has been relatively controversial. Part of the population sees it as a remarkable tool to control and improve energy efficiency. The other part of the population sees it as a sensitive tool, able to save and report critical information regarding household behaviour and life.

Ensuring privacy and security of smart meter data is a major challenge for energy companies, due to the degree of privacy and data protection that is mandated by GDPR. This is a difficult task for many reasons: first, the deregulation of the market in many EU countries created a lot of new energy data management companies including many Small and Medium-sized Enterprises (SMEs). SMEs, even more than big companies, have lots of difficulties with GDPR, and are missing a complete platform able to support them in being GDPR compliant concerning all the GDPR requirements. Second, utility companies often need to involve third service providers to collect, process and display to end-users the large amount of information sensed by smart meters.

The DEFeND platform is expected to provide a strong technical support for companies from the energy sector concerning achieving GDPR compliance. In particular, utility companies expect DEFeND to be able to identify their needs in terms of security and personal data. This can be done based on preliminary assessments to evaluate the structure and the nature of data, processes, roles of different controllers/processors of involved companies. DEFeND will be able also to identify decisive security measures thanks to its new methodological and technical approach. The challenge is to satisfy GDPR aspects for heterogeneous actors, with different needs, among customers, end-users, and third parties.

4.2 Challenges and DEFeND Benefits in the Healthcare Sector

GDPR defines health data as personal data relating to physical or mental health of a natural person, including provision of health care services, which reveal information concerning health status. Thus, medical information is high sensitive personal data (e.g. a disease, a disability). Due to the nature of this data, GDPR requires additional security measures for processing such information. Within those processes fundamental elements are to be considered such as the consent, quality of data, information to patients and confidentiality. The main legal basis for the treatment of sensitive data is the consent [3]. According to GDPR, this should be explicit and cannot be collected in unfair or fraudulent ways.

Within the DEFeND healthcare pilot, documentation referring to clinical-statistic sheets, entry authorization and urgency report will be considered. In the related processes, patients must be informed of the existence of these files, related purposes, possible recipients of information, the identity and address of maintainers and the possibility of exercising their rights. It is mandatory, in each health centre, the existence of an information sheet, at disposal of the patient, where authorization for data processing can be requested. It includes, for instance, name of the professional, the centre where the patient has been treated, purposes, and should express the publication agreement of the clinical case directed to health professionals. The professional secret is mandatory and medical centres must adopt necessary measures to guarantee confidentiality and legal access procedures for staff members.

To guarantee the correct recollection and storage of all this documentation, a platform directly designed for the healthcare domain is needed. Thus, the DEFeND platform will be integrated in the hospital information system to help privacy officers of health centres to comply with GDPR. For example, consent management has been always a big issue due to the vast paperwork involved. Thus, it is needed to complement existing software for health records with a platform that allows, patients and the clinicians, to be sure regarding the correspondence among health data treatments and the consent given. DEFeND consortium is developing the platform in collaboration with data protection officers of hospitals. Privacy by design will be applied with the concrete needs of healthcare institutions and patients. DEFeND will grant patients, and their tutors, the actual exertion of rights regarding data concerning their health, which is stored usually in a distributed way over several centres.

5 Related Work

The next two Subsections describe the novelty of the DEFeND platform and its architecture compared respectively to the industry situation and the literature.

5.1 Industry Comparison

According to the 2018 Privacy Tech Vendor Report from IAAP [2], the number of vendors providing privacy management technologies has doubled in one year, and some of the existing ones have enhanced offerings with new services. Despite the remarkable increase in the market offering, the report highlights also: ''there is no single vendor that will automatically make an organization GDPR compliant'' [2].

Solutions are classified in the IAAP's report into 2 main categories: Privacy Program Management and Enterprise Privacy Management, considering overall business needs. The first are grouped into 6 subcategories: assessment managers, consent managers, data mapping, incident response, privacy information managers and website scanning. The second are grouped in 4 subcategories: activity monitoring, data discovery, de-identification/pseudonymity and enterprise communications. None of the listed vendors is able to provide solutions that cover all the 10 sub-categories. AvePoint is the most complete vendor according to IAAP's report, offering numerous solutions that provide functionalities covering all sub-categories except for the enterprise communications. Functionalities offered by the DEFeND platform also cover 9 subcategories: all except the privacy information management subcategory. Contrary to AvePoint, DEFeND provides organizations with the capability to employ 1 platform for all GDPR compliance issues, during GDPR assessment, implementation, monitoring and response.

Forrester [1] released a report evaluating the 12 most significant providers in the market of EU GDPR compliance and privacy management. Providers offer privacy management platforms supplying services across geographies and reporting capabilities associated to a dashboard. Platforms are evaluated against 10 criteria. One important conclusion of the report is that a functionality such as data discovery across systems, is a key feature to avoid bad consequences of doing such task manually (i.e. inaccuracies, guesswork), and increases assurance in terms of accountability. DEFeND supports this functionality via the Organization Data Collection module, where organizational data is collected and automatically transformed to a Data Assessment Model. In addition, Data Privacy Impact Assessments (DPIA) functionality is considered a powerful feature by Forrester's analysis. DEFeND uniquely integrates privacy-by-design approaches with DPIA, and threat analysis, at planning level to create a set of tools enabling organizations to develop new services and systems in accordance with GDPR.

5.2 Research Novelty

The DEFeND Platform has been conceptualised around three axes of privacy protection, i.e. Privacy By Design, Consent Management and Privacy Impact Assessment and Risk Management, all related to the general obligations for

controllers and processors for GDPR compliance. In the following paragraphs, we explain the novelties that DEFeND introduces in all these three areas.

Privacy by Design. Various methodologies and patterns have been developed to ensure that systems and services are designed with respect to privacy. Problem-based Security Requirements Elicitation (PresSuRE) uses problem diagrams to support modelling of functional requirements, where every functional requirement of each asset is related with possible threats and security requirements [6]. In [5], a privacy threat analysis framework for privacy requirements elicitation and selection is designed. Privacy threats were identified, related to DFD elements and prioritised through risk assessment. Privacy Safeguard (PriS) [8], a privacy requirement engineering methodology, considers privacy requirements as organizational goals and uses privacy-process patterns to describe the impact of privacy goals to the affected organizational processes. A threat based approach to elicit privacy requirements, LINDDUN, is proposed by [5], which includes a systematic methodology and catalogue of privacy related threat tree patterns. The authors propose a mapping of privacy threat types to system components that are modelled with Data Flow Diagrams (DFDs). Once privacy threat types are identified, then are further refined with the help of privacy threat tree patterns specifically developed for each threat type. Finally, authors present a mapping of privacy requirements to existing Privacy Enhancing Technologies (PETs) in order to support analysts that are not experts in privacy technologies. The PRIPARE (PReparing Industry to Privacy by Design by supporting its Application in REsearch) methodology [7] is the result of a European Union funded project, which aims to integrate existing practices and research proposals on privacy engineering. It contains 7 phases enabling analysts to consider privacy issues.

The DEFeND platform advances the above state-of-the-art by facilitating organizations to implement a privacy management approach, which takes into account Privacy by Design, enabling them to (re)design their processes with respect to their privacy requirements, at an operational level. In other words, the DEFeND platform integrates privacy recommendations and suggestions on implementing privacy requirements from the early stage of service and software development. Moreover, such privacy recommendations and suggestions are assigned to agents, but without further justification of whether the agents can be trusted to take them, they remain just assumptions, which may prove wrong and lead to privacy breaches [12]. Trust-based concepts enable the developer to identify trust relationships and to analyse the identified trust relationships so that trust assumptions regarding privacy are valid [13]. Therefore, the DEFeND project facilitates further trust analysis which is required in order to justify that privacy requirements will be met by the suggested privacy implementations.

Consent Management. Research studies have demonstrated that obtaining user consent is difficult. First, the mechanism used widely for obtaining user consent is privacy policies and notices, however users do not read them [10]. Hence, consent becomes invalid and not informed [15]. Further, even if users read the privacy policies, their understanding is hindered by the legal and technical terminology and the difficulty to follow long texts [4]. Several more factors

contribute to this situation making the obtained consent not informed [15]. Considering data subjects have the right to revoke their consent at any time, organizations should provide the flexibility to them to withdraw consent as easily as they gave it, making the ''rights management process'' as simple as possible.

The DEFeND platform 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 and Risk Management. Risk management is based on the experience and knowledge of best practice methods. International risk management standards are used to support risks or threats identification, as well as to assess their probabilities. To structure the process of risk assessment, there are various attempts to develop ontologies for general risk assessments [9].

Privacy Impact Assessments (PIAs) can be used to identify and reduce privacy risks of projects. The UK Information Commissioner Office (ICO) has developed a set of steps and principles of the code of practice for conducting privacy impact assessment. The code explains the key principles behind a PIA and recommends that a PIA should be undertaken for any project that will either involve the use of personal data or have other impact on the privacy of individuals. The DEFeND platform advances 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 standards. This analysis will be performed in a easy and user-friendly interface, and it will not need a specific knowledge and expertise in security and/or risk analysis to be performed.

6 Conclusions

This work presents the architecture of the platform developed within the Data gov-Ernance For supportiNg gDpr (DEFeND)[1] EU project, and discusses challenges and preliminary benefits of its application to healthcare and energy sectors.

The aim of the DEFeND platform is to support organizations in achieving compliance with the European General Data Protection Regulation (GDPR), by following a Privacy by Design approach. Obtaining GDPR compliance for organizations is a very complex, difficult and expensive task. This is due to the vastness and complexity of GDPR, covering many data protection aspects, and requiring organizations to adopt multiple heterogeneous security measures, remaining abstract and not providing organizations with clear, concrete technological indications. In the industry and in the literature, there are many tools and prototypes able to cover only a very reduced set of GDPR aspects. Thus, the DEFeND platform covers this gap, by proposing a comprehensive platform satisfying the full complexity of GDPR, through an architectural design able to integrate and reuse the most relevant peculiarities of heterogeneous avail-

able tools, making them to collaborate as architectural components providing organizations with a Privacy by Design workflow.

Finally, in this paper we discuss also challenges and preliminary benefits in the application of the DEFeND platform to healthcare and energy sectors. As future work, we will evaluate the platform also within banking and public administration pilots in real and realistic scenarios.

Acknowledgments. This work was partially supported by the DEFeND EU project, funded from the European Unions Horizon 2020 research and innovation programme under grant agreement No 787068.

References

1. The forrester new wave, https://www.forrester.com/report/The%20Forrester%20New%20Wave%20GDPR%20And%20Privacy%20Management%20Software%20Q4%202018/-/E-RES142698
2. Privacy tech vendor report, https://iapp.org/resources/article/2018-privacy-tech-vendor-report/
3. Regulation 2016/679 and Directive 95/46/EC (GDPR) of the EU on the processing of personal data and on the free movement of such data (2016), https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en
4. Capistrano, E.P.S., Chen, J.V.: Information privacy policies: The effects of policy characteristics and online experience. Computer Standards & Interfaces (2015)
5. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering Journal (2011)
6. Fabender, S., Heisel, M., Meis, R.: Problem-based security requirements elicitation and refinement with pressure (2015)
7. Garcia: Pripare privacy by design methodology handbook. Tech. rep. (2015)
8. Kalloniatis, C., Belsis, P., Gritzalis, S.: A soft computing approach for privacy requirements engineering: The pris framework. Applied Soft Computing (2011)
9. Mayer, N., Dubois, E., Matulevicius, R., Heymans, P.: Towards a measurement framework for security risk management.
10. McDonald, A.M., Cranor, L.F.: The cost of reading privacy policies. ISJLP (2008)
11. Mouratidis, H., Argyropoulos, N., Shei, S.: Security requirements engineering for cloud computing: The secure tropos approach (2016)
12. Pavlidis, M., Mouratidis, H., Gonzalez-Perez, C., Kalloniatis, C.: In: CRiSIS 2015
13. Pavlidis, M., Mouratidis, H., Islam, S.: Modelling security using trust based concepts. International Journal of Secure Software Engineering (IJSSE) (2012)
14. Piras, L., Dellagiacoma, D., Perini, A., Susi, A., Giorgini, P., Mylopoulos, J.: Design Thinking and Acceptance Requirements for Designing Gamified Software. In: 13th Intern. Confer. on Research Challenges in Information Science (RCIS). IEEE (2019)
15. Tsohou, A., Kosta, E.: Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. Computer Law & Sec. Review (2017)
16. Zheng, J., Gao, D.W., Lin, L.: Smart meters in smart grid: An overview. In: 2013 IEEE Green Technologies Conference (GreenTech) (2013)