SN Computer Science (2020) 1:217
https://doi.org/10.1007/s42979-020-00218-8

SURVEY ARTICLE

Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects

Renata M. de Carvalho[1] · Camillo Del Prete[2] · Yod Samuel Martin[3] · Rosa M. Araujo Rivero[4] · Melek Önen[5] · Francesco Paolo Schiavo[6] · Ángel Cuevas Rumín[7] · Haralambos Mouratidis[8] · Juan C. Yelmo[3] · Maria N. Koukovini[9]

Received: 6 January 2020 / Accepted: 8 June 2020 / Published online: 27 June 2020

Abstract
Confidence in information and communication technology services and systems is crucial for the digital society which we live in, but this confidence is not possible without privacy-enhancing tools and technologies, nor without risks management frameworks that guarantee privacy, data protection, and secure digital identities. This paper provides information on ongoing and recent developments in this area in the European Union (EU) space. We start by providing an overview of EU's General Data Protection Regulation (GDPR) and proceed by identifying challenges concerning GDPR implementation, either technical or organizational. For this, we consider the work currently being done by a set of EU projects on the H2020 DS-08-2017 topic, namely BPR4GDPR, DEFeND, SMOOTH, PDP4E, PAPAYA and PoSeID-on, which address and aim at providing specific, operational solutions for the identified challenges. We briefly present these solutions and discuss the ways in which the projects cooperate and complement each other. Finally, we identify guidelines for further research.

Keywords GDPR · Privacy · Data protection · Digital identities

Introduction

The digital revolution raised a severe issue on personal data protection. The Internet of things, cloud computing, big data, social media and machine learning enable organizations to collect large amounts of personal data. However, together with all the benefits that such technologies bring, the probability of (deliberate or accidental) misuse of citizens' data also increases mostly due to lack of control over management and privacy issues of citizen data. Data breaches pose a serious risk for all organizations and have direct implications to individuals since the latter lose the confidentiality of their data and their anonymity.

The European Union, first through the Data Protection Directive [1], then through the General Data Protection Regulation [2], has recognized the importance for citizens of the value of data privacy and the necessity for the privacy-enabled management of personal data.

The European Commission, in order to facilitate the implementation of the GDPR, funded several projects through the programme Horizon 2020—Secure societies—Protecting freedom and security of Europe and its citizens—Cybersecurity PPP: Privacy, Data Protection and Digital Identities [3].

Our research focuses on the following projects:

– Business Process Re-engineering and functional toolkit for GDPR compliance (BPR4GDPR)
– Data Governance for Supporting GDPR (DEFeND)

This article is part of the topical collection "Privacy, Data Protection and Digital Identity" guest edited by Fernando Boavida, Andrea Praitano and Georgios V. Lioudakis.

✉ Renata M. de Carvalho
r.medeiros.de.carvalho@tue.nl

1 Eindhoven University of Technology, Eindhoven, The Netherlands
2 Maticmind, Vimodrone, Italy
3 Universidad Politecnica de Madrid, Madrid, Spain
4 Centre Tecnològic de Catalunya, Barcelona, Spain
5 EURECOM, Biot, France
6 Italian Ministry of Economy and Finances, Rome, Italy
7 Universidad Carlos III de Madrid, Madrid, Spain
8 University of Brighton, Brighton, UK
9 ICT abovo P.C., Athina, Greece

- GDPR Compliance Cloud Platform for Micro Enterprises (SMOOTH)
- Methods and tools for GDPR compliance through Privacy and Data Protection Engineering (PDP4E)
- PlAtform for PrivAcY preserving data Analytics (PAPAYA)
- Protection and control of Secured Information by means of a privacy enhanced Dashboard (PoSeID-on)

These projects aim at finding solutions for "both technological as well as organizational challenges for organizations which have to implement novelties such as the right to data portability, the right to be forgotten, data protection impact assessments and the various implementations of the principle of accountability" [4].

This document highlights how these projects face common challenges and adopt complementary solutions for protecting citizens' personal data and privacy.

The remainder of the paper is organized as follows. "General Data Protection Regulation (GDPR)" section gives an overview of the General Data Protection Regulation (GDPR) and presents the rights of data subjects. "Challenges Concerning GDPR" section discusses the challenges faced to implement GDPR, whereas the proposed solutions are explained in "Solutions Proposed by Each Research Project" section. Finally, "Conclusion" section summarizes the proposed solutions and identifies guidelines for future work.

General Data Protection Regulation (GDPR)

Our society is benefiting significantly from internet connectivity and leverage digitalization to make more efficient the ways in which we communicate, interact and we work with one another. As previously mentioned, this growing dependence on technology, however, also brings new forms of risks and exposure for citizens, economies and administrations, and has forced the necessity for data protection rights. The EU *General Data Protection Regulation (GDPR)* is intended to establish a consolidated framework to guide commercial use of personal data and to strengthen data protection for EU citizens. The GDPR is being implemented to standardize and modernize data protection laws related to the Internet, social networks and digital market, and to protect and empower all EU individuals when it comes to the privacy of their data.

The assigned control of personal data to individuals in the EU with the addition of new rights for EU data subjects is impacting the manner in which organizations are dealing with personal information. GDPR has altered the ways for collecting and managing personal information, including the definition of new roles in organizations handling with data subjects, such as:

- *Data controller* "is a natural or legal person, public authority, or body that alone or jointly with others determines the purposed and means of the processing of personal data. The technical and organizational measures to ensure and demonstrate that data processing is performed according with GDPR is the role of the data controller".
- *Data processor* "is the natural legal person, public authority or body that processed personal data on behalf of the controller. They need to meet the standards set forth by the controllers with the sufficient guaranties".
- *Data protection officer* is the role designated by controller and processor whose responsibility is overseeing an organization's data protection strategy and implementation, for ensuring that it is complying with the GDPR's requirements.

These new data subject rights (see Fig. 1) comprise new information assets like:

- *Access information about personal data* the individual has the right to obtain data from controllers concerning his/her processing of personal data, and, when it is the case, access to such personal data and obtaining information on, among other things, the purpose of processing, the categories of personal data, the third parties to whom personal data has been disclosed, etc.;
- *Right to be forgotten* An EU data subject has the right to obtain the erasure of personal data concerning him/her without undue delay;
- *Automated individual decision-making, including profiling* The data subject has the right to not being subject to a decision based on automated processing. The profiling of a person for the purpose of analysing or predicting behaviours or preferences is regulated by law;
- *Consent* Personal data cannot be processed without consent unless expressly allowed by law. Consent must be freely given, specific, informed, unambiguous and pre-ticked boxes or inactivity do not constitute consent;
- *Data portability* This is the right to receive personal data provided by the individual to a controller, in a structured, commonly used and machine-readable format, to be transferable to another controller if certain circumstances apply;
- *Time limits* Personal data shall not be kept for longer than necessary for the purposes for which the personal data is processed, but may be stored for longer periods in case of public interest, and scientific or historical research purposes.

In essence, GDPR presents risks and opportunities, given that best practices and technology-enhanced information workflows can enable organizations to be more responsive, agile and efficient. In order to adapt to the GDPR, standards

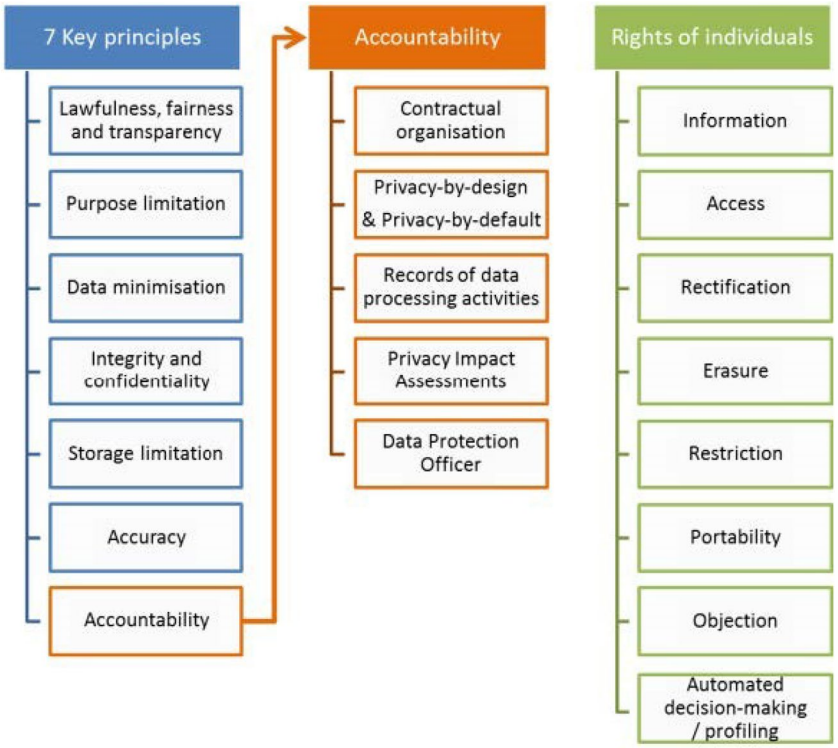

Fig. 1 Data subject rights according to GDPR

for personal information management have to be created that can serve as a basis for organizations to be more efficient and GDPR compliant.

In consequence, GDPR exponentially increases data security responsibilities and risks for organizations, and a strategy is required to cope with GDPR and other regulations. Information technology plays a key role in data governance, systems strategies and management, to accomplish personal data requirements, enhancing information security and developing breach-awareness capabilities aligned with those of the organization.

We may conclude that GDPR compliance is a vehicle for leveraging data workflow improvements, for optimizing day-to-day activities, and for generating greater added value to customers and stakeholders. Implementing the new best practices, new work models and new technologies as the ones that we will be presenting in this paper can make a difference.

Challenges Concerning GDPR

Since its implementation on May 25th, 2018, awareness around GDPR and its impact is growing. For example, if we compare the number of data breach notifications to the European data protection authorities since the GDPR implementation started, in January 2019 we had around 41k vs. 89k in May 2019 (about > 30%) [5]. Therefore, the demand for solutions that could help organizations improve compliance with the law is also increasing.

Apart from the mandate for GDPR compliance—and the non-negligible financial penalties, compliance is motivated also by the market needs, particularly the growing people awareness and their increasing demand to companies for the protection of their information [6]. For example, the 2015 TalkTalk privacy breach resulted in over 100.000 customers' loss and costed around £60m [7].

However, organizations declare difficulties in GDPR provisions' implementation, despite the resources and money spent, whereas particular problems are faced as regards to the new requirements introduced by GDPR. The challenges, either technical or organizational, include, among others: interpretation of GDPR requirements; operational adaptation towards privacy-aware and compliant business practices; holistic data views and processing actions inventory; enforcement of security means; management of the relations with third parties and the data subjects, and enforcement of rights thereof; last but not least, significant resources are required and, whereas big companies may have money and resources to invest, both human and monetary, this does not necessarily apply to SMEs.

GDPR provides a bunch of data protection principles, data subject rights and obligations for data controllers and processors. However, as a legal text, it does not constrain the potential technical solutions, and leaves open the means that can be applied to achieve compliance. The GDPR itself

provides for the creation of supplementary quasi-, co- and self-regulation (European Data Protection Board guidelines, European Court of Justice rulings, codes of conduct, corporate binding policies, certifications); these, indeed, reveal the complexity associated to GDPR compliance and the need for resources that provide an appropriate interpretation.

The projects we are presenting here address such lack of specific, operational solutions which respond to the challenges and legal innovations posed by GDPR, by providing systematic methods, detailed techniques, and software tools that guide the compliance process in a broad sense. All of them take into special consideration the constraints their target users may face, e.g. the budget limitations that different types of SMEs can afford when addressing GDPR compliance, or the lack of savvy in the field by mainstream engineers, consultants and individual entrepreneurs. Such users shall be able to follow the guidance yielded by the projects, apply their methods and use their tools without being experts on privacy and data protection topics, leveraging automated support when possible. Moreover, recognizing the need for specialized solutions, and the failure of a one-size-fits-all approach, the software tools created by these projects are characterized by their modularity, loose coupling and extensibility, so that different parts can be reused and taken advantage of in different scenarios. In the following, we characterize some of the specific challenges faced by each of the above-mentioned projects.

Business Process Re-engineering and Functional Toolkit for GDPR Compliance (BPR4GDPR)

BPR4GDPR[1] identified the need for a new GDPR compliance paradigm, by providing the tools and methodologies that will significantly facilitate the implementation of the appropriate technical and organizational measures, particularly by SMEs, to ensure that data collection and processing is performed in accordance with the GDPR. The compliance approach has to consist in automatically re-engineering workflows, being business processes or low-level service compositions, so that they become compliant by design, whereas enforcement will be supported by an easy to deploy "compliance toolkit", providing the fundamental common functions for cryptography, access management and enforcement of data subjects' rights. Further, the overall organizational compliance and underlying systems' behaviour should be governed by a comprehensive policy-based access and usage control framework, conceived on the basis of the GDPR and managing all requirements thereof. Finally, solutions have to be on the Cloud, therefore providing for compliance-as-a-service (CaaS).

Data Governance for Supporting GDPR (DEFeND)

GDPR provides for strict principles and obligations, and recognizes a handful of rights to individuals that must be anticipated by organizations.

In addition, the security aspects, the anonymization/pseudonymization of data, the data breaches' identification and subsequent notifications, the international data transfers or the legal grounds (such as consent) are complex legal aspects that must be handled by organizations. Although the market is full of companies offering their services and tools for GDPR compliance, such solutions are mostly focused on providing generic approaches and frameworks that allow organizations to evaluate their current GDPR readiness level and propose some generic guidelines for moving towards compliance. They do not, however, provide specific methods, techniques and tools to tackle the above challenges. As a result, the above challenges remain. It is therefore important, as indicated by the EU call "Secure societies—Protecting freedom and security of Europe and its citizens" (topic DS-08-2017: Cybersecurity PPP: Privacy, Data Protection and Digital Identities), "to develop tools and methods to assist organizations to implement GDPR...". DEFeND[2] main challenge is to build a platform to assist organizations to implement GDPR.

GDPR Compliance Cloud Platform for Micro Enterprises (SMOOTH)

In 2018, there were more than 25 million SMEs in the Europe-28, and overall SMEs accounted for:

- Almost all EU non-financial sector (99.8%),
- 2/3 of total EU-28 employment (66.6%),
- Slightly less than 3/5 (56.4%) of the value added generated by the non-financial business sector.

Micro SMEs (referred to as MEnts from now on in this paper), are by far the most common type of SME, accounting for 93.0% of all enterprises and 93.2% of all SMEs in the non-financial business sector.

MEnts are in particular, a sub-category of SMEs which presents a major risk of failing in adopting the GDPR. These MEnts are companies with less than 10 employees including self-employed people and constitute one of the major contributors to the European economy and societal well-being. In 2018, they were responsible for 29.7% of total employment in the non-financial business sector, while small- and medium-sized SMEs accounted, respectively, for 21% and 16.8% of total non-financial business sector employment.

[1] https://www.bpr4gdpr.eu/.

[2] https://www.defendproject.eu/.

While public bodies and large corporations have the resources and/or expertize required for efficiently adopting the GDPR, MEnts may struggle to do so due to their lack of resources and/or expertize.

Hence, MEnts represent the vast majority of European enterprises with a huge impact on the European economy and employment. At the same time, MEnts are the most vulnerable entities in the adoption of the GDPR due to their lack of awareness, expertize and economic resources.

The adoption of the GDPR by MEnts in a smooth manner, without incurring unnecessary or unaffordable costs, is of vital importance to the EU global economy and constitutes the high level objective of the SMOOTH project.[3] Some elements that need to be addressed in order to achieve that objective are:

- Lack of data protection regulation awareness among MEnts,
- Clear explanation of the GDPR mandates affecting MEnts,
- Lack of affordable and simple solutions for MEnts addressing the GDPR mandates.

Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering (PDP4E)

PDP4E[4] focuses on the challenges posed by current approaches to privacy and data protection in the development process. Despite the momentum gained by privacy and data protection in the recent years from both the regulatory and the organizational arena, that has not been translated into their application through systematic engineering practice. In particular, the introduction of privacy and data protection aspects into products, systems and services is usually approached from one of the following perspectives, all of which are disconnected from engineering as such:

- The "privacy by policy" approach [8] focuses on compliance with legal regulations. Such compliance is usually addressed by the organization's legal staff, who directly convey legal constraints to the engineers in charge of developing the system. However, there is an "impedance mismatch" between the language, tools and processes used by legal and engineering teams, which effectively preclude the proper integration of privacy and data protection aspects into the development life cycle.
- The privacy by design (PbD) principles [9] seek that privacy and data protection be considered in a user-centric (i.e. data subject centric) approach throughout all the stages of the systems development lifecycle (SDLC). Despite some attempts to operationalize PbD principles into more detailed guidance [10], they remain too abstract and detached from the engineering practice [11] which makes them difficult to realize and even foster the user of PbD as a buzzword without real grounds. If any, engineers tend to consider privacy only from an operational security perspective, reducing it to confidentiality and access control at runtime.
- The "privacy by architecture" approach relies on the implementation of privacy-enhancing technologies (PETs) to minimize the personally identifiable information processed [8]. However, the introduction of most of these PETs in the implementation of products still requires the involvement of privacy-savvy engineers, who often need to craft tailored solutions on a case-by-case basis, instead of having non-privacy experts methodically introduce such technical solutions.
- Finally, privacy program management (PPM) and privacy enterprise management (PEM) [12] can simplify the consideration of privacy by corporate processes, but they do not target the activities of engineers during the development process, nor do they even integrate with the engineers' usual tools.

PlAtform for PrivAcY Preserving Data Analytics (PAPAYA)

Traditionally deployed data encryption techniques are unfortunately not suitable to the big data paradigm where data is continuously processed via data analytics techniques ranging from simple statistics (such as sum, mean and standard deviation) to more sophisticated machine learning techniques (such as linear regression and neural networks). Indeed, whenever standard encryption techniques are used, they prevent third-party servers to operate over the encrypted data. One solution is to give the key to these untrusted servers to decrypt the data, but confidentiality is no more ensured. It is therefore of paramount importance to design privacy preserving primitives that would be compatible with the underlying data analytics technology. More specifically, PAPAYA [5] advocates for solutions that enable to perform analytics operations on encrypted data without decrypting it in order to be compliant with the GDPR.

While homomorphic encryption succeeds in resolving the conflict between data encryption and data analytics, the actual technology is not ready yet to be applied as a generic privacy protection solution because of its prohibitive computational cost. Therefore, there is a strong need for practical privacy enhancing technologies that would be tailored to the

[3] https://smoothplatform.eu/.

[4] https://www.pdp4e-project.eu/.

[5] https://www.papaya-project.eu/.

underlying data mining techniques. Another challenge when designing a privacy preserving data analytics service is the multiplicity of data sources. While the ability to learn an accurate model entirely depends on the diversity of training data, recent privacy-related regulations inhibit data producers from sharing (sensitive) data with third parties. In this regard, privacy preserving data analytics should consider the case of data coming from multiple sources while enabling collaborative analytics without compromising the privacy of the different data owners involved in the collaboration.

Protection and Control of Secured Information by Means of a Privacy Enhanced Dashboard (PoSeID-on)

The widespread use of digital services has led to user concerns on privacy and on the processing of their personal information by data processors and third parties. This, in turn, leads to national and/or regional legislation, such as EU's General Data Protection Regulation (GDPR), that aim at providing legal assurances in what concerns the protection of personal identifiable information (PII). On the other hand, technological development continues to deliver frameworks tools, and applications that demand PII user data in order to fulfil user needs in a large variety of areas, from public administration to sensitive individual health data. In this context, demand for ways of protecting and controlling PII information has never been so high.

The goal of the PoSeID-on Project ("Protection and control of Secured Information by means of a privacy enhanced Dashboard")[6] is to develop a transparent ecosystem for personal data protection, in line with GDPR with respect to digital security. The project aims to design, implement and validate a privacy-enhancing dashboard for personal data protection, a platform that manages all the personal data transactions between a data subject (owner of personal data) and private or public entities acting as data controllers or data processors. All relevant information shall be made available to users via a user-friendly web dashboard that allows them to track personal identifiable information (PII), manage PII access permissions and view the risk level stemming from their data exposure. In order to reduce identity fraud and protect the privacy of users, access to the dashboard is to be made available through eID accounts only, in line with the eIDAS regulation [13].

[6] https://www.poseidon-h2020.eu.

Solutions Proposed by Each Research Project

According to the data protection by design principles required/established by GDPR, which draws from earlier privacy by design principles, privacy and data protection should be proactively embedded in the systems-to-be since their inception and throughout their development (rather than as an afterthought or, even worse, as a mere reaction to data breaches). Thus, our projects introduce privacy in a variety of activities and tools that cover the whole span of the systems development lifecycle. Some (PDP4E, SMOOTH, PAPAYA) mostly focus on the design time, while others (DEFeND, BPR4GDPR, POSEIDON) are also targeting runtime and operation. All in all, they encompass a broad range of processes and activities: requirements operationalization and instantiation (PDP4E), modelling (DEFeND, PDP4E, BPR4GDPR), process engineering (BPR4GDPR, PDP4E), risk management (POSEIDON, PDP4E), verification and validation (BPR4GDPR, SMOOTH, PDP4E), runtime monitoring (BPR4GDPR) and refactoring (BPR4GDPR, PDP4E).

Besides, although each of the said projects is addressing its own, individual goals, common topics can be traced among them, as they all address some of the crucial challenges posed by GDPR:

- *Data and process inventory* GDPR requires that most organizations keep a registry of the data processing activities they carry out, including data categories, data subjects affected, etc. Even when such registry is not compulsory (e.g. for small enterprises), it is still pivotal for other activities (e.g. it is quite difficult to address data subject portability requests if there is no such inventory of personal data categories). Hence, features are provided to elicit, map and analyse data (DEFeND, SMOOTH, PDP4E) and processes (BPR4GDPR), to model data flows (SMOOTH, PDP4E) and business processes (BPR4GDPR), even by dynamically discovering process on runtime (BPR4GDPR).
- *Consent management* GDPR requires that organizations are able to prove the nature of the consent they have got to process personal data. Together with other lawful basis for processing (e.g. contracts, legitimate interests), other GDPR principles (which deal with collection, storage and purpose limitation) and obligations to limit disclosure, it may be difficult to ensure that processing activities is lawful at all times. With that aim, many of these projects try to bridge data subject interests with organization processes, by providing features that support consent and preference management (DEFeND, BPR4GDPR) on the one hand; and policy,

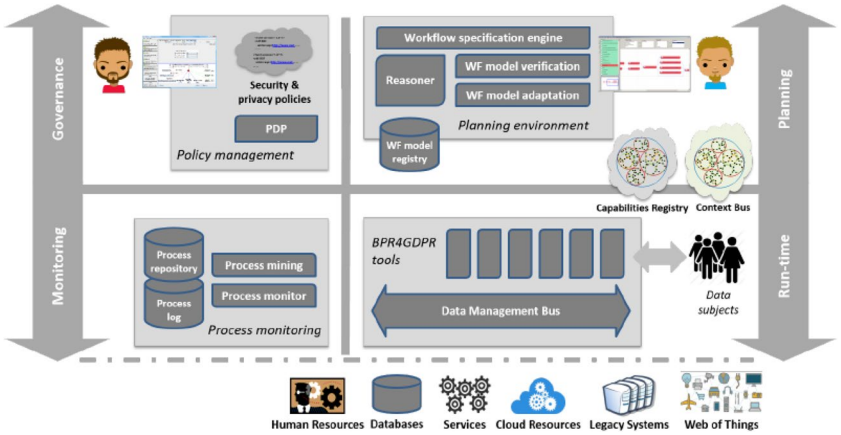

Fig. 2 BPR4GDPR architecture

data, permission and data subject rights management and enforcement (BPR4GDPR, POSEIDON) on the other one. Dashboards are particularly recognized (PAPAYA, BPR4GDPR, POSEIDON) as an appropriate pattern to address the complexity of dynamic consent management from the data subject's side.

- *Encryption measures* GDPR requires that security and data protection technical measures are applied and enforced. In this respect, several projects (DEFeND, PAPAYA, BPR4GDPR) address encryption-based protection measures (e.g. privacy-preserving encryption, anonymization or cryptography-based access control).
- *Distributed data processors* GDPR establishes obligations regarding data processors which may perform data processing activities on behalf of the data controllers (which are ultimately responsible for that). Several projects (BPR4GDR, PAPAYA, POSEIDON, SMOOTH) take especially into account such distribution of data processing activities provided "as a Service" among several organizations. Such distribution paradigm is even brought to the solutions provided by the projects themselves (PAPAYA, BPR4GDPR, SMOOTH), by sticking to a "compliance as a service" approach that fosters the distribution of the different software modules developed.
- *Accountability* GDPR compliance not only requires abiding by the measures prescribed there, but also being able to demonstrate that they have been effectively implemented and responsibly adopted. This concept, known as the accountability principle, requires keeping evidence of the measures taken and processes carried out, and it is also being addressed by some projects (POSEIDON, PDP4E).

Next, we detail the solutions planned by each project and to what extent they solve the challenges mentioned in the previous section.

BPR4GDPR

In order to cover its functional needs towards GDPR compliance and cope with the operational phases, BPR4GDPR has specified the system architecture highlighted in Fig. 2. As illustrated, the BPR4GDPR architecture is divided in four "quadrants", reflecting different groups of functionalities. In the following, the main principles and technical ideas are summarized.

Governance provides all functions related to policy management, representing the Policy Decision Point (PDP) of the system. In BPR4GDPR, policies hold a dual role: (1) they provide the means for system governance, in the sense that they set the rules that regulate the operation of BPR4GDPR components; (2) they comprise the knowledge base that feeds the procedure of process reengineering, towards by design compliant process models. To this end, BPR4GDPR develops a comprehensive Policy-based Access and Usage Control framework, tailored for the needs of highly distributed environments, involving multiple stakeholders, even in cross-border scenarios. The ground technology is the academic work described in [14], along with the respective software prototype, whereas policies are grounded on the compliance ontology, providing a high-level codification of GDPR into concepts that need to be taken into consideration by the policy framework.

Planning concerns the specification of workflow models and their verification as regards compliance with the GDPR, and their subsequent transformation, if needed, so that they become compliant by design. The first step in this direction is facilitated by tools allowing their description in a way that effectively guides their execution, while also being expressive enough to capture associated provisions; these tools are grounded upon prior academic work of BPR4GDPR researchers [15]. Further, in order to automatically incorporate policies as part of workflow design, the BPR4GDPR approach involves sophisticated means for the evaluation

of process specifications against a number of compliance aspects. Their main aim is to control access to, usage of and flow of information and prevent illegitimate activity, as well as to determine whether critical tasks are properly included and, if not, impose their execution.

Monitoring deals with process mining and monitoring with the aim to identify discrepancies between compliant and actual behaviour. To this end, BPR4GDPR implements a Privacy-Aware Process Mining Framework, based on mature technology brought by its partners, particularly ProM[7] [16, 17]. The approach is primarily based on two concepts: streaming process mining, that allows analysing real-time data in order to detect problems, anomalies and potential frauds; the concept drift issue, calling for solutions for change detection and continuous update, in order to handle situations where new factors/requirements render the process model out-of-date and in need to be adapted/improved.

Finally, in order to facilitate the deployment of appropriate technical measures, as required by the GDPR, *Run-time* provides the means for the run-time system operation, particularly in terms of policy enforcement, data management, privacy-enhancing tools, and interaction with data subjects. In this context, the project provides a set of functional components addressing common needs of stakeholders. This so-called Compliance Toolkit consists of modular functions that, fostering "plug and play" to the extent possible, will be easy to deploy, easy to configure and easy to integrate within an organization's ICT environment, while they will be automatically incorporated to process chains, as a result of re-engineering. The toolkit's modules fall into three families:

- *Privacy-enhancing technologies*, particularly cryptographic tools, devised for data and communications confidentiality, anonymization and pseudonymization, as well as enforcement of access rights by cryptographic means [18].
- *Data management tools* that, by means of data access and usage management, provide for controlling data handling, including retention and storage, pre- and post-processing, etc. A core position is held by the Data Management Bus (Fig. 1), comprising the main Policy Enforcement Point (PEP).
- *User-centred tools*, providing for the enforcement of the data subjects' rights, including information and notification, consent, and consideration of own preferences as regards data handling.

[7] http://www.promtools.org/.

DEFeND

Although the market is full of companies offering their services and tools for GDPR compliance, such solutions are mostly focused on providing generic approaches and frameworks that allow organizations to evaluate their current GDPR readiness level and propose some generic guidelines for moving towards compliance. They do not, however, provide specific methods, techniques and tools to tackle the above challenges. As a result, the above challenges remain. It is therefore important, as indicated by the EU call *Secure societies—Protecting freedom and security of Europe and its citizens (topic DS-08-2017: Cybersecurity PPP: Privacy, Data Protection and Digital Identities)*, "to develop tools and methods to assist organizations to implement GDPR".

We strongly believe the proposed Data Governance for Supporting GDPR (DEFeND) Platform will tackle these challenges therefore significantly contributing to the objectives of the call, through the development of tools and methods integrated into a platform that will provide solutions to the above challenges and support continuous GDPR compliance.

The main aim of the DEFeND project is to deliver an innovative data privacy governance platform, which will facilitate scoping and processing of data and data breach management and will support organizations towards GDPR compliance.

Organizations, in order to comply with the GDPR, have to implement in their processes, at a very low-level, different tools, solutions and processes, so privacy is inherently integrated in these. Therefore, it is important that DEFeND provides a solution that not only supports compliance of the relevant GDPR articles, but also fulfils special characteristics of needs that organizations might have. That way DEFeND goes beyond current products that offer general solutions and need special expertize and effort in order to cover the requirements of the organizations (by adapting the general solutions to the special needs of the organizations).

Another important aim for DEFeND is to be budget-available. We found many of the current solutions available in the market are too expensive for SMEs and require a high-level of expertize in order to adapt them. Therefore, it is important that DEFeND is adaptable enough so that organizations with budget restrictions can still make use of it. We plan to achieve this by following a modular strategy that provides different services to users and supports both planning and operational stages. This allows two innovative characteristics: on the one hand, the solutions are more specific to the needs of the organization and, on the other hand, the modules of DEFeND could be extended with new solutions. Another aim of DEFeND is to support not only organizations to comply with GDPR but consultants, (legal

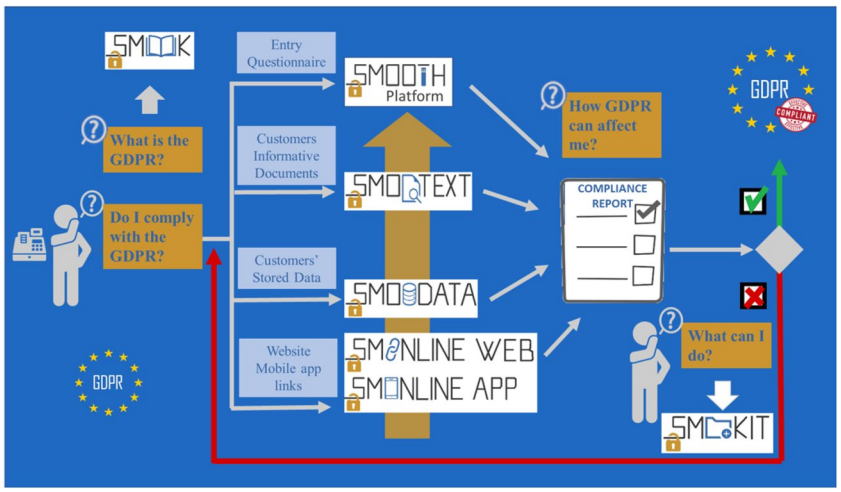

Fig. 3 Overview of the SMOOTH platform

and/or technical) to use it as part of their consultancy services to clients seeking GDPR compliance.

To achieve the above aims, the project focuses on providing a realistic and useful solution that deals with the main research challenges mentioned above, through 7 objectives:

1. Design and development of a successful, market-oriented, platform to support organizations towards GDPR compliance
2. Develop a modular solution that cover different aspects of the GDPR
3. Automated methods and techniques to elicit, map and analyse data that organizations hold for individuals
4. Advanced modelling languages and methodologies for privacy-by-design and data protection management
5. Specification, management and enforcement of personal data consent
6. Integrated encryption and anonymization solutions for GDPR
7. Deployment and validation of the DEFeND platform in real operational environments

SMOOTH

Solutions targeting MEnts to help them to adopt the GDPR should be simple, economically affordable, reliable and of general purpose so that they can be used independently of their business context. SMOOTH aims at implementing a cloud-based platform that meets all these requirements and automatically assess the compliance of MENTs regarding basic elements of the GDPR that affect most of them. Figure 3 outlines the SMOOTH platform.

The SMOOTH platform is being implemented in a modular approach comprising a front-end and a back-end. The front-end performs the interactions with the MEnts in order to: (1) get all the contextual information and resources (documents) required for running GDPR compliance validation tests, (2) deliver the GDPR compliance report in a simple, constructive and reliable format. The back-end integrates the technologies implementing the automatic assessment of compliance with the main elements of the GDPR impacting the MEnts. The compliance report is to be generated in the back-end based on the results obtained from the automatic assessment process. Following, we detail these components.

SMOOTH Front-End

MEnts access the SMOOTH platform through a registration/subscription process where they have to fill an entry questionnaire. The questionnaire captures contextual information about the MEnt business, such as its data protection background, the personal information that is collecting from its customers/providers (if any) and the data protection mechanisms currently in place (if any). This information is highly valuable to the algorithms performing the compliance analysis in the back-end.

Once the registration phase is completed, the platform front-end will offer MEnts an intuitive and assisted process to upload the resources required to carry out the automatic compliance assessment process in the back-end. An initial list of such resources includes: (1) currently used informative documents (e.g. informed consent, terms of use, cookie policy for MEnts with online presence); (2) a sample of the customers'/providers information repository (e.g. files, database) where (personal) data is stored; (3) URL of the website(s); and (4) link to the mobile app. It is important to note that depending on the MEnt under analysis some of these resources may not be available.

It should also be stressed that SMOOTH will use the customers' data repository only for the purpose of generating the compliance report. The data analysis will happen in real

time and once the compliance report is delivered, all data sample from the MEnt will be removed from the platform. In any case, due to the analysis process, the SMOOTH platform becomes a data processor; therefore, MEnts, being the data controllers, will have to sign an online contract for letting the SMOOTH platform process their data. This contract will be signed the first time MEnts access the SMOOTH platform. This way, we guarantee that SMOOTH is itself compliant with the GDPR.

Finally, the front-end will be the interface to deliver the GDPR compliance report generated in the platform back-end. This report will use a plain and simple language in a constructive tone to expose the failures in the GDPR compliance, in an order of importance, along with appropriate guidance for their resolution.

Back-End

The goal of the SMOOTH back-end is to automatically produce a compliance report against the main basic elements of the GDPR affecting MEnts. The back-end uses as input the information provided in the registration process and the resources uploaded by the MEnts to the platform. The back-end is formed by three modules each of them analysing specific resources type. The output generated by these modules will be consolidated to produce the GDPR compliance report. Following, we describe the modules comprising the SMOOTH platform back-end.

1. *SMOOTEXT* This module analyses the content of the (offline or online) documents used by MEnts to inform customers of the personal data collected and the purpose for which they are used as well as the procedures that customers should follow to execute their rights (e.g. access or erasure) as data subjects according to the GDPR. We refer to those documents such as informed consent, terms of use, privacy policies, cookie policies, etc. This module validates if the conditions and elements required by the GDPR are included in the documents. In addition, it extracts from the analysed documents the list of personal data items that the MEnt declares to be storing. As a result, it reports whether any of the GDPR elements analysed is not properly addressed or not adequately described in the documents (e.g. the document does not include text to inform the user how it can execute its right to data erasure, language used is very complex syntax, etc).
2. *SMOODATA* This module analyses the personal information that MEnts are storing using as input the sample of customers' and providers' information repository uploaded by the MEnts. The module assesses if the MEnt has sufficient permission to store the information that it is actually storing. That is, whether the MEnts are only storing the personal data items declared in the consent documents (analysed by the previous module) or is storing personal data (by mistake) non-agreed by users in the consent documents with the customer personal data. The module also identifies the presence of" Sensitive Personal Data" in the data repository. This type of data requires a special treatment (e.g. sensitive personal data must be encrypted).
3. *SMONLINE* The informative documents and data collected by MEnts through their websites and mobile apps are mostly covered in SMOOTEXT, which analyses documents such as websites/mobile apps terms of use, consent requests, cookies policies, or privacy policies and SMOODATA, which analyses the data repositories used to store the information collected by the MEnts's websites or mobile apps. This module analyses the data flows from websites (SMONLINE WEB) and mobile apps (SMONLINE APP) to find potential privacy leaks. In the case of websites and mobile apps, the management of personal information may also involve third party companies different than the MEnts (e.g. advertising, tracking and social network integration). Hence, this module emphasizes the analysis of personal information leaks to third party companies from MEnts' websites and/or mobile apps. This information will be used together with the output of SMOOTEXT for validating if: (1) the website visitors are being informed of the collection of their (personal) data (e.g. website activity) by third party companies, (2) the terms of use informs the visitors how to execute their rights as data subjects, and (3) the visitors are asked their consent for sharing information with the identified third parties and for what purposes. In addition, this module analyses the potential use of personal data under monetization strategies (i.e. online advertising). This module is also reporting the list of third party organizations retrieving user information from the MEnts websites/mobile apps (which may constitute privacy leakage events compromising users' privacy).

Each of the above modules has an added value in its own right. Focusing on specific aspects of the GDPR, each module could well apply to larger organizations beyond the context of MEnts. In SMOOTH, the three modules will be integrated together to create the core of the SMOOTH platform. The output generated by each module will be processed and combined together to create the final GDPR compliance report to be delivered to the MEnts.

PDP4E

As previously explained, privacy and data protection aspects are usually dealt with from perspectives which, despite

providing valuable contributions, are not aligned with systematic engineering practice. This makes engineers consider privacy as an unfamiliar aspect they often ignore [19]. Nonetheless, in order to ensure that privacy and data protection features are effectively embedded in the products, systems and services, it seems reasonable to directly involve those who are responsible for creating and developing them—that is, put the engineers in the loop. Any legal innovation (e.g. data minimization principle, right to be forgotten, data protection impact assessment, or accountability, to name just a few) needs to go along with systematic guidance to engineers, so as to ensure that it is effectively implemented [20]. This idea follows the "code is law" aphorism, in that features implemented by software products has practical implications of what is allowed to do as much as the legal regulation.

Hence, PDP4E claims that engineers must be *endowed with methodological and technological tools* to systematically apply privacy of data protection principles so as to comply with the regulatory framework. These methods and tools should allow for other, competing requirements and system constraints, and they must especially bear in mind that the savvy and effort to apply them by non-privacy-experts should be taken to a minimum, by being aligned with the engineers' expertize. In order to pay effective consideration to privacy and data protection, engineers must be endowed with tools that map data protection principles, data subject rights, and controller obligations, onto engineering terms such as backlog items, database structures, business process models or deployment architectures.

Thus, PDP4E fosters the production of privacy and data protection methods and tools that *integrate within the large heritage of software and systems engineering*, which have long amassed a substantial wisdom that is methodically and systematically applied by engineers in their daily work—and which might well be taken advantage of for privacy and data protection as well. PDP4E vouches the seamless inclusion of privacy and data protection functions into general-purpose software and system engineering tools of customary use by engineers (as recommended by ENISA [21]), to support that privacy and data protection be embedded throughout the methods and workflows followed by engineers in the SDLC. This represents a "shift left" in the application of privacy and data protection, from the Op[eration]s towards the Dev[elopement] activities. That way, PDP4E results populate the field of *Privacy and Data Protection Engineering*, which "pursues systematic approaches for the inception and application of privacy-oriented solutions throughout systems and software development processes" [22] and which precisely revolves around methods and tools employed by engineers [23].

It shall be noted that this approach implicitly considers a *honest but reckless engineer*, who is willing to introduce privacy and data protection into their developments, but lacks the expertize or the resource (be it monetary or time) to appropriately address them. Likewise, we also remark that this implies that the organizations developing products are willing to cooperate to achieve privacy and data protection, and they are committed to protecting data subjects from attacks to their privacy, even if these might yield some benefit to the organization itself. That is, the organization assumes being in charge of protecting the rights and freedoms of the data subjects on their behalf, even if might defy some (illegitimate) business ambitions. This approach is not so peculiar indeed, as it is already applied in other fields (e.g. Occupational Safety and Health where organizations must look after the work-related risks of their employees). All in all, this Privacy and Data Protection Engineering approach does not prevent organizations holding personal data from intentionally violating privacy and data protection regulations and principles if they are willing to do so, but lowers the practical barriers they may be facing to reach the compliance they have voluntarily assumed and committed to achieve.

PDP4E is providing a set of systematic, economical, engineering methods and tools (as opposed to mere legal regulation, void principles, informal craftsmanship or managerial procedures) that introduce privacy and data protection issues throughout the disciplines of the systems development lifecycle (SDLC), leveraging the wisdom of software and systems engineering and integrating within existent, general-purpose, engineering methods and tools. In particular, PDP4E is addressing four disciplines, viz. risk management, requirements engineering, model-driven design and systems assurance.

- The *Risk Management* discipline addresses potential negative effects of uncertain events. In PDP4E, these mostly refer to the impact on the individuals' (i.e. data subjects') rights and freedoms derived from the personal data processing activities carried out by an organization (data controller), in the context of a Privacy and Data Protection Impact Assessment (PIA / DPIA). Nonetheless, following a multilateral security approach, PDP4E also gives appropriate consideration to security risks, business risks and risks related to data processors (vendors that process data on behalf of the data controller under a contract). Typical risk management concepts (e.g. assets, threats, vulnerabilities, impacts, countermeasures or controls) are handled by the PDP4E risk management method, which builds on previous risk assessment methods (LINDDUN [24] and STRIDE [25]) and the use of data flow diagrams (DFDs) to model how personal data flows across different data processing activities and organizations (i.e. data controllers and processors).
- The *Requirements Engineering* discipline allows analysing, managing and verifying that a product, system

or service meets the needs posed by a variety of stakeholders. In PDP4E, privacy and data protection requirements arising from legal texts, industry standards and generic privacy goals (e.g. unlinkability, transparency, and intervenability [26]) are handled as templates of non-functional requirements (NFRs), which can only make sense if they are parameterized and instantiated within the specific context of the endeavour at hand (i.e. the specification of each project's functional requirements). In PDP4E, this process is addressed through the successive refinement of abstract needs into operational requirements, and the use of a lightweight version of the "problem frames" approach initially proposed by PROPAN [27].

– The *Model-Driven Design* discipline allows representing a system under development from different perspectives, so as to support engineers in moving from an abstract understanding of the system to a fine-grained, detailed design; and eventually verifying that the system models match the desired properties. PDP4E method proposes that models of the system-to-be be enriched with properties that respond to privacy and data protection specific features. For instance, structural models (dealing with data types, attributes and relationships) can include further properties to determine which data is personal, whether it is sensitive, upon what basis it was collected, and how long it can be retained. Procedural models (e.g. dataflows) can represent the processes that deal with personal data, the processing operations it is being subject to, how data flows from one operation to another, for what purpose it is being used, and who is authorized to access it. And architectural models (representing components and their deployment) can represent who stores and processes personal data and under which jurisdiction. But model-driven design goes beyond a merely descriptive approach: it can be leveraged for data mapping and inventory activities (i.e. identifying and categorizing the personal data that will be processed by the system), analysis and reasoning about the most appropriate design solutions regarding privacy and data protection (through the systematic application of privacy design strategies, tactics and patterns [28]), and generation of model-based tests that help verify the application of access control mechanisms.
– The discipline of *Systems Assurance* focuses on the actions that must be arranged and executed to achieve and ensure the confidence that a system abides by some given requirements. Compliance with modern privacy regulatory frameworks requires not only sticking to the corresponding legally binding obligations, but also being able to demonstrate that appropriate actions have been taken throughout the development process. Thus, systems assurance becomes key to support privacy principles such as accountability, transparency and intervenability. PDP4E provides a formal model of the regulatory framework (in particular, GDPR and its interpretation through related quasi-, co- and self-regulations) as a method that includes required processes and relevant relations between one another, roles that carry them out, plus their input and output products. Then, during the development of a project, generated artefacts are captured that provide evidences, which can be traced to specific requirements posed by the regulatory framework, so that, all in all, and through a logical argumentation process, compliance with the regulation can be claimed. In order to support that assurance process, PDP4E also provides reusable argumentation patterns that act as templates of typical techniques to achieve and justify compliance.

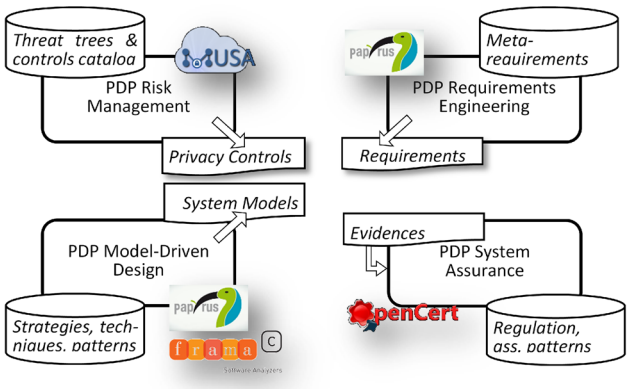

Fig. 4 PDP4E toolset

This approach is realized into a set of interrelated but loosely coupled Privacy and Data Protection Engineering tools that PDP4E is producing (Fig. 4, and which leverage and extend general purpose software and system engineering tools already in the context of each of the said disciplines. Thus, the privacy and data protection risk management tool is a new version of a previous security-management tool called MUSA, the requirements engineering and the model-driven design tools are extensions of Papyrus (a modular model-driven engineering framework), together with some ancillary tools implemented on the source code analysis tool Frama-C, and the assurance tool draws from the OpenCert assurance framework. All the tools that PDP4E is creating are equipped with knowledge bases (of different types, depending on the respective discipline), whose contents can be instantiated during a development process. These knowledge bases capture best privacy and data protection practice and make them ready to be used from engineering tools. Likewise, all the tools rely on model-based approaches and produce models of one or another type (controls, requirements, system

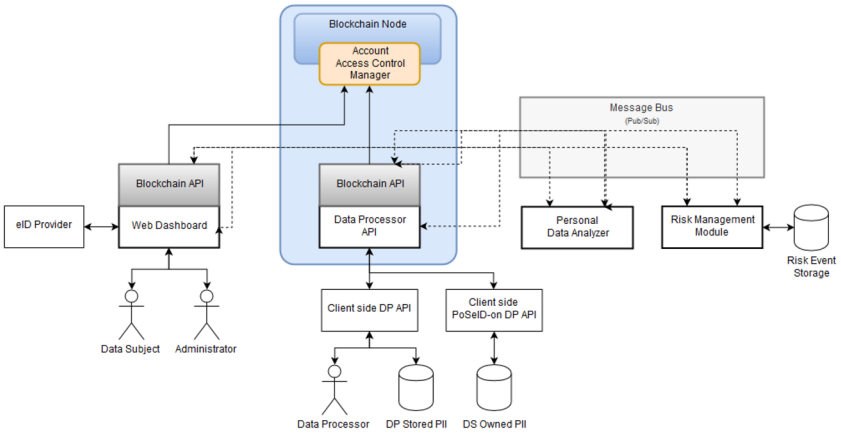

Fig. 5 PoSeID-on architecture

structure, processes and architecture, argumentations, among others). The results of the different tools are also related: the risk management and the requirements engineering tools provide complementary views (risk-oriented and goal-driven, respectively) of the attributes that shall be met and validated by the design; the assurance tool captures artefacts produced by other tools as evidences for compliance, etc.

PAPAYA

The main objective of PAPAYA is to design and develop a *platform of privacy preserving analytics modules that allows the outsourcing of analytics operations into untrusted cloud servers* while protecting the privacy of the data. Thanks to these newly developed privacy preserving analytics modules, stakeholders will be able to ensure their clients' privacy (and be compliant with the GDPR) while extracting valuable and meaningful information from the analysed data.

In particular, PAPAYA develops novel privacy preserving neural network classification primitives that are based on partially homomorphic encryption, secure two-party computation or fully homomorphic encryption. A privacy preserving collaborative training solution based on differential privacy is also being implemented. Furthermore, the problem of privacy preserving counting and privacy preserving trajectory clustering are investigated.

The PAPAYA framework contains components that will be running in the cloud environment (such as privacy preserving machine learning services, auditing services and others), and components that will be running on the client side (such as the Data Subject toolbox which will provide means for end-user privacy and usability of the platform). To facilitate user experience and enable data subjects and data controllers to exercise their rights over their data and control what is disclosed to third parties, the platform will provide dashboards for the different actors featuring, e.g. usable visualizations and auditing components.

PoSeID-on

The PoSeID-on solution is based on innovative technologies such as blockchain [29], smart contracts and cloud computing, that provide targeted benefits for end-users, potentially enabling them to manage personal data and data access authorizations in an easy, secure and auditable way. Additionally, it helps both public and private entities to identify new business opportunities, to be compliant with GDPR while processing personal data, as well as to undergo a substantial ICT-driven transformation, which will ensure higher security of end-user's data. PoSeID-on also impacts society as a whole, as it leads to increased trust in the digital market, in addition to supporting fundamental rights in the digital society.

Through smart contracts, the project aims to meet the need of data confidentiality, inviolability, and access control for data subjects. Through the blockchain technology, references to PII shall be managed and exchanged securely. The blockchain technology was selected due to two main reasons. First and foremost, there was the need to maintain an irrevocable record of PII transactions, including permissions handling and all kinds of operations involving PII processing, for providing full control to PII owners, for accountability, and for legal assurances. On the other hand, there was need to allow multiple entities to share data and to contribute to data processing, without relinquishing control over their own databases, or without relying on a central datastore. By agreeing to participate in the PoSeID-on system, users benefit from full control over their PII, and third parties can provide an auditable ledger of all their PII-related operations to users and regulators. Moreover, it should be highlighted that no PII is ever stored in the blockchain, that only stores information on permissions and on PII handling.

Figure 5 illustrates the overall PoSeID-on architecture, identifying the various system components.

Table 1 lists the conceptual components and the respective short description.

Table 1 PoSeID-on architecture components

PoSeID-on conceptual architecture components	Brief description
Data subjects, data processors, and administrators	Primary target of PoSeID-on platform end-users
Dashboard	Interface for data subjects and administrators
Data processor API	Access point for data processors to send/receive requests
Client-side data processor API	Connector to data processor's internal information systems
Permissioned blockchain and smart contracts	Blockchain implementation where only authorized parties can propose changes. Serves as a back-end for PII access management within the PoSeID-on platform.
Blockchain API	Abstraction layer that allows modules to access and interact with the blockchain.
Risk management module	Detects operational anomalies which may translate to security and privacy risks.
Personal data analyser	Detect and evaluate privacy risks within PII transactions
eID provider	Authenticates users in the PoSeID-on platform
Data subjects' PII repository	PoSeID-on's storage for PII owned by the data subject (e.g. not belonging to a data processor, introduced manually by the data subject into PoSeID-on)
Message bus	Messaging module for PoSeID-on's components communication

It should be noted that, from the perspective of PoSeID-on, data controllers (entities that determine the purposes, conditions and means for the processing of PII) and data processors (the entities that process PII on behalf of data controllers) are treated in the exact same way, as these functionalities often reside in the same system.

The platform developed by the project is now being assessed in four different pilot deployments (in Italy, France, Spain and Malta), in public, private and mixed contexts. Specifically, the Italian pilot aims at enhancing e-services for public officials, the Spanish pilot aims to improve e-Government services for the citizens of Santander, the Maltese pilot focuses on helping businesses to better sponsor and offer their services to customers, and the French pilot is aimed at simplifying e-services for French citizens. Initially, pilots involve a basic, limited set of users, to be enlarged during the evaluation phase. The pilots run in a controlled environment in order to simulate real-life services and conditions.

Conclusion

With the rapid growth of information exchange, including personal data, which became easier and faster with the advent of the internet, individuals are providing their data knowingly and, sometimes, unknowingly for many different purposes. As the Internet has an inherited nature of being frontier-less, which enables the free flow of data across countries, there is need to protect citizens' personal data and privacy. To this end, the European Union acted first through the Data Protection Directive and then through the General Data Protection Regulation (GDPR). However, implementing GDPR also poses many challenges, which were discussed in this paper.

In order to contribute to solving some of those challenges, the EU research projects considered in this paper proposed several solutions. As it is not yet feasible to address all the issues, each project has its own target public and/or focuses on some specific aspects of GDPR. Table 2 summarizes which aspects of GDPR are addressed by each project. Although not final, the solutions proposed and discussed in this paper will already provide means for: (1) allowing citizens to track their personal data, manage permissions and view the risk of data exposure; (2) dealing with encryption of data that enables analytics operations to be performed without exposure of the data; (3) providing methods to assist organizations in implementing security and legal aspects; (4) enabling privacy and data protection to be considered in the development process from different perspectives; (5) caring about the impacts (specially financially) on SMEs and MEnts in adopting GDPR; and (6) supporting SMEs to become GDPR-compliant by automatically re-engineering their processes to enforce GDPR.

Despite the work being carried out, several other aspects of GDPR remain open and were not discussed in this paper, such as purpose limitation, data minimization and storage limitation. As these are also important to protect citizens' privacy, they will be addressed by future work/projects. Moreover, ongoing and future work to be carried out in the scope of the concerned projects will address piloting and assessment of the proposed solutions, and integration of complementary solutions. For this, continued cooperation between the projects is being pursued.

Table 2 Summary indicating which aspects of GDPR are addressed by each project

Challenges	BPR4GDPR	DEFeND	PAPAYA	PDP4E	PoSeID-on	SMOOTH
Data and process inventory						
Elicit, map and analyse data	✗	✓	✗	✓	✓	✓
Elicit, map and analyse processes	✓	✓	✗	✓	✗	✗
Model data flows	✗	✓	✗	✓	✗	✓
Model business processes	✓	✓	✗	✓	✗	✗
Discover process on runtime	✓	✗	✗	✗	✗	✗
Consent management						
Consent and preference management	✓	✓	✓*	✗	✓	✗
Policy, data permission and data subject right management	✓	✓	P	✗	✓	✗
Dashboard	✓	✓	✓	✗	✓	✗
Data protection measures						
Anonymization	✓	✓	✓	✗	✓	✗
Data encryption	✓	✓	✓	✗	✓	✗
Cryptography based access control	✗	✓	✓	✗	✓	✗
Privacy preserving data processing	✓	✓	✓	✓	✓	✓
Distributed data processing						
Distributed processing as a service	✓	✗	✓	✗	✓	✓
Compliance as a service	✓	✗	✓	✗	✗	✓
Accountability						
Evidence of measures	✗	✓	P	✓	✓	✗

(✓) means the aspect is part of the project's solution; (✗) means it is not; and (P) indicates that the aspect is partially covered. Specifically, (✓*) means only preference management

Acknowledgements The authors have received funding within: the BPR4GDPR project from the European Union's Horizon 2020 research and innovation programme under Grant agreement No. 787149; the PDP4E project from the European Union's Horizon 2020 research and innovation programme under Grant agreement No. 787034; SMOOTH project (G.A. no 786741) from the European Union (EU) under the Digital Security Focus Area of the Horizon 2020 (H2020) Innovation Action programme; the PAPAYA project from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 786767; the DEFeND project from the European Union's Horizon 2020 research and innovation programme under Grant agreement No. 787068; the PoSeID-on project from the European Union's Horizon 2020 research and innovation programme under Grant agreement No. 786713.

References

1. European Union. Directive 95/46/EC of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046. Accessed 17 Dec 2019.
2. European Union. Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed 17 Dec 2019.
3. European Union. Cybersecurity ppp: privacy, data protection, digital identities id: Ds-08-2017. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/ds-08-2017. Accessed 17 Dec 2019.
4. European Union. Horizon 2020 work programme 2016–2017 14. secure societies—protecting freedom and security of Europe and its citizens (part 14—page 74). https://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf. Accessed 17 Dec 2019.
5. European Commission. Infographic: GDPR in numbers (25 January 2019, 22 May 2019). https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en. Accessed 17 Dec 2019.

6. European Commission Directorate-General for Communication. Flash eurobarometer 443: e-privacy. https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG. Accessed 17 Dec 2019.
7. Farrell S. Talktalk counts costs of cyber-attack. https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave. Accessed 17 Dec 2019.
8. Spiekermann S, Cranor LF. Engineering privacy. IEEE Trans Softw Eng. 2009;35(1):67–82.
9. Cavoukian A, et al. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada. 2009. p. 5.
10. Cavoukian A. Operationalizing privacy by design: the Ontario smart grid case study. Information and Privacy Commissioner, Ontario, Canada; 2011.
11. Birnhack M, Toch E, Hadar I. Privacy mindset, technological mindset. Jurimetrics. 2014;55:1–71.
12. International Association of Privacy Professionals (IAPP). 2019 privacy tech vendor report. https://iapp.org/media/pdf/resource_center/2019TechVendorReport.pdf.
13. European Union. Regulation (EU) no 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisery%3AOJ.L_.2014.257.01.0073.01.ENG. Accessed 17 Dec 2019.
14. Papagiannakopoulou Eugenia I. Semantic access control model for distributed environments. Ph.D. Thesis, National Technical University of Athens, 2014.
15. Koukovini Maria N. Inherent privacy awareness in service-oriented architectures. Ph.D. Thesis, National Technical University of Athens, 2014.
16. van der Aalst WMP, van Dongen BF, Günther CW, Rozinat A, Verbeek HMW, Weijters AJMM. Prom: the process mining toolkit. BPM (Demos). 2009;489:2.
17. Mans RS, van der Aalst WMP, Verbeek HMW. Supporting process mining workflows with rapidprom. In: BPM 2014 Demos, vol. 1295. CEUR-WS.org. 2014. pp. 56–60.
18. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: 2007 IEEE symposium on security and privacy (SP '07), May 2007. pp. 321–334.
19. Balebako R, Marsh A, Lin J, Hong JI, Cranor L. The privacy and security behaviors of smartphone app developers. 2014. p. 2 .
20. European Commission. The future of privacy—article 29 data protection working party and working party on police and justice. 2009. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf. Accessed 19 Dec 2019.
21. Danezis G, Domingo-Ferrer J, Hansen M, Hoepman J-H, Métayer DL, Tirtea R, Schiffner S. Privacy and data protection by design—from policy to engineering. 2014. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design. Accessed 19 Dec 2019.
22. García YSM, del Álamo Ramiro JM. A metamodel for privacy engineering methods. In: Proceedings of the 3rd international workshop on privacy engineering co-located with 38th IEEE symposium on security and privacy (S&P 2017), vol. 1873, CEUR Workshop Proceedings. 2017. pp. 41–48.
23. Gürses S, del Alamo JM. Privacy engineering: shaping an emerging field of research and practice. IEEE Secur Priv. 2016;14(2):40–6.
24. Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir Eng. 2011;16(1):3–32.
25. Shostack A. Threat modeling: designing for security. New York: Wiley; 2014.
26. Hansen M, Jensen M, Rost M. Protection goals for privacy engineering. In: 2015 IEEE security and privacy workshops, May 2015. pp. 159–166.
27. Beckers K, Faßbender S, Heisel M, Meis R. A problem-based approach for computer-aided privacy threat identification. In: Bart P, Demosthenes I, editors. Privacy technologies and policy. Heidelberg: Berlin; 2014. p. 1–16.
28. Hoepman J-H. Privacy design strategies. In: Cuppens-Boulahia N, Cuppens F, Jajodia S, El Kalam AA, Sans T, editors. ICT systems security and privacy protection. Berlin: Springer; 2014. p. 446–59.
29. Stallings W. A blockchain tutorial. Inter Prot J. 2017;20(3):2–24.