Privacy Data Management and Awareness for Public Administrations: A Case Study from the Healthcare Domain

Vasiliki Diamantopoulou[1(✉)], Konstantinos Angelopoulos[1], Julian Flake[2], Andrea Praitano[3], José Francisco Ruiz[4], Jan Jürjens[2,5], Michalis Pavlidis[1], Dimitri Bonutto[6], Andrès Castillo Sanz[7], Haralambos Mouratidis[1], Javier García Robles[4], and Alberto Eugenio Tozzi[6]

[1] University of Brighton, Brighton, UK
{v.diamantopoulou,k.angelopoulos,
m.pavlidis,h.mouratidis}@brighton.ac.uk
[2] Fraunhofer-Institute for Software and Systems Engineering, Dortmund, Germany
{julian.flake,jan.juerjens}@isst.fraunhofer.de
[3] Business-e, Rome, Italy
andrea.praitano@business-e.it
[4] Atos, Madrid, Spain
{jose.ruizr,javier.garciar}@atos.net
[5] University of Koblenz-Landau, Koblenz, Germany
[6] Ospedale Pediatrico Bambino Gesù, Rome, Italy
{dimitri.bonutto,albertoeugenio.tozzi}@opbg.net
[7] International University of La Rioja UNIR, Madrid, Spain
andres.castillo@unir.net

Abstract. Development of Information Systems that ensure privacy is a challenging task that spans various fields such as technology, law and policy. Reports of recent privacy infringements indicate that we are far from not only achieving privacy but also from applying Privacy by Design principles. This is due to lack of holistic methods and tools which should enable to understand privacy issues, incorporate appropriate privacy controls during design-time and create and enforce a privacy policy during run-time. To address these issues, we present VisiOn Privacy Platform which provides holistic privacy management throughout the whole information system lifecycle. It contains a privacy aware process that is supported by a software platform and enables Data Controllers to ensure privacy and Data Subjects to gain control of their data, by participating in the privacy policy formulation. A case study from the healthcare domain is used to demonstrate the platform's benefits.

Keywords: Privacy management · Data protection · Privacy level agreement · eHealth · Telemedicine · VisiOn Privacy Platform

E. Schweighofer et al. (Eds.): APF 2017, LNCS 10518, pp. 192–209, 2017.
DOI: 10.1007/978-3-319-67280-9_11

1 Introduction

The rapid development and the advances in Information and Communication Technologies (ICT) have led to their adoption by organisations, enabling them to transform their services to e-services, increasing their efficiency, productivity and growth [12]. Emphasis is given on security and privacy of the Information Technology (IT) systems when they are used for the management of personal data. During the development and operation of IT systems, security and privacy properties should be satisfied. This is even more imperative when IT systems are used by data controllers who work and manage critical types of personal data (i.e. sensitive data), for example, health-related ones.

The adoption of IT systems by the healthcare sector can also demonstrate substantial benefits, e.g., cost reduction, improved quality of care, promotion of evidence based medicine, record keeping, mobility [15], offering of efficient and real-time services to patients, flexibility, and patient safety [22]. However, the transition from paper-based health records to Electronic Health Records (EHR) lurks new challenges related to the secure transmission and privacy-handling of data, since health information is considered to be one of the most confidential types of personal information [14]. Health data exposed in the electronic environment is vulnerable to security and privacy threats [13].

The necessity for the privacy-enabled management of personal data is also reflected in the General Data Protection Regulation (GDPR) [5], which aims to protect the data subjects' interests, imposing data controllers to ensure data subjects' privacy and providing them the ownership and control of their data. Moreover, a recent research [4] regarding the European citizens' opinion for their attitude to data protection revealed that 69% of them are concerned that their personal data may be used for a purpose other than the one it was collected for. Other studies [19] have indicated that patients are reluctant to share their health information but for direct clinical care.

Data controllers should ensure secure management of their IT systems but also this should be communicated to the data subjects who are obliged to provide their personal data to use the provided e-services. Additionally, data subjects should be aware of their privacy rights so they can decide and declare their preferences regarding the management of their personal data.

This paper proposes the VisiOn Privacy Platform (VPP), an outcome of a H2020 European Project that provides privacy protection for electronic provided services by Public Administrations, which can be adequately applied in the healthcare domain. The adoption of this holistic, platform-supported approach improves privacy regarding the e-services in the following perspectives: (a) it enhances user's trust and confidence when using e-services, by exploiting existing software engineering approaches and combining them with modelling languages to analyse trust relationships between data controllers and data subjects (i.e. hospitals and patients), which could negatively affect the adoption of such services that the data controllers provide; (b) it improves transparency, by imposing accountability to data controllers, regarding protection of data subjects' information; (c) it builds confidence between the data controllers and sub-

jects, since it provides a new type of Privacy Management system that allows the latter to take control over the data they provide in order to take advantage of the e-services; (d) it adapts data controller's privacy protection policies to each data subject's privacy preferences and introduces the concept of Privacy Level Agreement (PLA), a formal digital contract between data controllers and data subjects. A PLA presents the results of the analysis of the privacy threats, vulnerabilities and trust relationships of data controllers' IT systems, whilst complying with laws and regulations. Moreover, the structure of the PLA allows data controllers to elicit data subjects' privacy requirements, and eventually provides feedback regarding the data sharing policies of the data controllers.

The remainder of the paper is structured as follows: Sect. 2 discusses the state of the art while Sect. 3 presents the functionalities and the architecture of VPP. Section 4 illustrates our work with a real-world case study. Finally, Sect. 5 concludes the paper and raises issues for further research.

2 State of the Art

The concept of VPP encapsulates various aspects, namely the protection of privacy issues, the privacy awareness that arises to data subjects, the identification of privacy and security requirements from multiple perspectives and the customisation of privacy policies, based on individuals' privacy preferences.

The idea of an agreed, standardised way for web sites to communicate with users regarding their privacy policies presented in a standard machine-readable format has been introduced by the Platform of Privacy Preferences (P3P) Project [24]. This standard facilitates web browsers and other user agents to interpret privacy policies on behalf of their users, providing them directions in order to decide when to exchange data with web sites. The limitation of P3P lies on the fact that it was designed for static environments where users' privacy preferences are not expected to change. Furthermore, P3P does not provide sufficient support for specifying privacy threats and vulnerabilities that might endanger the privacy needs. In [10] the authors propose an architecture that promotes the employment of privacy policies and preferences. They define and introduce the concept of the Privacy Controller Agent for collecting, storing and comparing service providers' privacy policies with the preferences specified by the users. However, this work, as opposed to VPP, does not provide an agreement between two entities (e.g., citizen and PA, patient and hospital) but rather an architecture to define privacy policies.

In the literature multiple approaches have been proposed for capturing privacy requirements systematically. The Privacy Safeguard (PriS) [18], a privacy requirements engineering methodology, incorporates privacy requirements into the system design process, where privacy requirements are modelled as organisational goals. Next, the Modelling and Analysis of Privacy-aware Systems (MAPaS) framework [7] models requirements for privacy-aware systems. The authors in [23] adopt the concepts of privacy-by-policy and privacy-by-architecture, and propose a three-sphere model of user privacy concerns, relating

it to system operations (i.e. data transfer, storage and processing). The authors in [11] propose a framework for privacy management and policies that addresses various organisational perspectives, focusing on how organisations should evaluate their own privacy policies. Differently than those works, VPP provides a holistic privacy management approach which is based on the Privacy by Design (PbD) principles, since it starts with the elicitation of the user privacy requirements and it ends with the provision of Public Administration online services.

The concept of PLA has been recently adopted by the research community as a standardised way for cloud providers to describe their data protection practices. More specifically, the Privacy Level Agreement Working Group of the Cloud Security Alliance has defined a PLA in the context of cloud services [8]. In the same direction, the authors in [9] have presented the concept of PLA focusing on the cloud environment while the PLA is considered as a formal way for the cloud providers to ensure that their privacy policy is communicated to the service consumers. However, these works are limited to privacy aspects of cloud provision without providing any support for the specification of user's (e.g., citizen, patient) preferences or the definition of privacy threats and vulnerabilities.

Finally, the recent development of quite a few commercial products highlights the need regarding the individuals' data protection. A repository provided by the Information Shield[1] contains all the necessary material to support companies and organisations in formalising or updating their privacy policies while maintaining them compliant with relevant laws and regulations, at national and international level. Nymity[2] supports organisations enabling them to demonstrate data privacy compliance, based on an accountability approach. 2B Advice[3] is a consulting services organisation, consisted of a group of companies which aims to offer data privacy advice, software solutions and certifications. Another software solution dedicated to data protection management is called Otris privacy[4]. This tool focuses on the planning, setting-up, operation and decommissioning of data processing methods. OneTrust[5] platform assists service providers to guarantee the data privacy compliance with the relevant regulations, laws and privacy policies to their clients. Contrary to these products, VPP conducts security and privacy analysis of the information systems of each service provider, which is reflected to each PLA, ensuring that the processes followed by the organisations are law compliant. This is achieved by including in our proposed platform a tool that allows to encode privacy laws and automates the law-compliance checks of the composed privacy management policies. Additionally, the aforementioned approaches compose privacy management policies ad-hoc, whereas in VPP are composed by the preferences of the service consumers.

[1] https://informationshield.com/.
[2] https://www.nymity.com.
[3] https://www.2b-advice.com.
[4] https://www.otris.com/products/data-protection-management/.
[5] https://onetrust.com.

Another commercial solution for data protection is the TRUSTe[6] platform, which directs on Data Privacy Management (DPM), enabling users to control a set of provided technology-driven solutions in order to manage potential privacy challenges. Similarly, Disconnect[7] is a commercial software that facilitates users to easily understand the websites' privacy policies and realise how websites are handling their data. The common characteristic of the aforementioned two commercial solutions is that they focus on the better analysis and comprehension of each privacy policy, protecting user from actions that will put their personal data in danger. The approach that the VPP follows is based on the privacy preferences elicitations from both sides - service providers and service consumers - allowing the development of personalised PLAs, according to them.

3 The VisiOn Privacy Platform

3.1 The VisiOn Privacy Platform Functionalities

VPP supports the analysis of privacy issues from different perspectives (i.e. organisational, business-process, threat, and trust). It provides a holistic approach, covering all the potential aspects that influence and, consequently, shape the relationship in terms of trust between data subjects and online services provided by a data controller. VPP distinguishes two roles: data controller and data subjects. The data subject uses VPP's functionalities during run-time only, i.e. while using a service carried out by the data controller. The data controller uses VPP's functionalities during both, design-time and run-time of a system.

Data Controller's Functionalities. During design-time, the data controller/data processor uses VPP to capture security and privacy requirements of their systems by modelling and analysing the data controller's/data processor' system or service under planning, from different perspectives: (i) potential threats to the data controller's systems and its environment that lead to security and privacy issues are captured and countermeasures to mitigate these risks are identified; (ii) trust relationships between the data controller and third party providers are modelled and analysed in order to realise whether these relationships endanger transparency and accountability from data subjects' perspective; (iii) the socio-technical environment of the data controller's/data processor's systems is captured by models of interactions between human and non-human actors. These models capture goals the actors try to achieve and information that is processed to achieve the goals; (iv) procedural models of business processes, enriched with security related information, which can act as blueprints to define executable business process models containing supplementary security related information; (v) once the requirements, with a special focus on the security and privacy aspect, are captured, the data controller's/data processor's system designer can

[6] https://www.truste.com.
[7] https://disconnect.me/icons.

specify the details of the system under planning, by using a standard modelling language. The resulting specification models can be complemented with privacy and security related constraints the models have to comply with, while identified non-compliances are reported. The reports can be used by the system designers to refine their system specifications to finally meet the privacy specifications.

All models and analysis results enhance the data controller's/data processor's comprehension of the privacy and security issues, regardless of the expertise level and the technical knowledge of the data controller's employee, supporting the visual analysis of privacy and security issues at different levels and perspectives.

In addition to this design cycle support, VPP offers functionalities that prepare the actual use of VPP during run-time. The data controller/data processor uses VPP to create questionnaires that are filled by data subjects once the system is in production. This allows the data controller to capture each data subject's privacy preferences, which are used to create data access policies and, finally, the PLA. VPP supports the data controller/data processor in creating questionnaires, by suggesting suitable questions, automatically derived from system models. Furthermore, machine-readable representations of data protection legislations are fed into the system by the data controller/data processor, in order to specify policies that must be fulfilled by the system. This, together with a checklist questionnaire, allows the data controller to self-assess its compliance with relevant laws and regulations. Non-compliance issues are reported and can be resolved before the system or service under planning is released. As an additional preparatory step before the system or service under planning is released, the data controller/data processor fills an additional questionnaire to provide information required for the evaluation of data subjects' personal data.

During run-time, the data controller's system uses VPP to evaluate data access requests against the privacy policies reflecting the data subjects' privacy preferences. The data controller's/data processor's system can use VPP for the actual enforcement of data access policies. The data controller/data processor uses VPP directly to monitor the system's compliance with the data processing policies that reflect the data subject's privacy preferences during run-time.

Data Subject's Functionalities. Data subjects are supported by VPP during run-time in different ways. In the first place, data subjects interact with VPP to define and update their privacy preferences related to their personal data, by answering the aforementioned questionnaire, where they define if and how they wish their data to be processed. These privacy preferences are input to data access policies and PLAs. Data subjects can view their personal PLA, which furthermore contains visual representation of the systems involved in the processing of the data subjects' data, and the results of system analysis and law compliance checks performed by the data controller. All information contained in the PLA aims to raise transparency of the data processing and therefore the trust in lawful processing of the data subjects' personal data. Moreover, VPP provides useful insights to the data subjects regarding the value of their personal data. Thus, realising the value of their data, data subjects are able to choose

what data they wish to share and with whom, which might lead to the need to modify their personal privacy preferences. Finally, VPP enables data subjects to monitor issued access requests related to their personal data, the data access decisions and enforcements.

All the aforementioned functionalities aim to raise the data subjects' awareness of how their data is processed and of any potential threats, giving them all the necessary information to decide the level of data sharing. Moreover, VPP enables the interaction between data controllers and data subjects, respecting thus the latter's privacy rights, as the GDPR requests. Finally, VPP enables data controllers, and also data processors or data protection officers, to communicate - in a semi-automated way - the identified data breach(es) (Article 34 of [5]).

3.2 The Vision Privacy Platform Architecture

After defining the functionalities of VPP, the logical architecture of the platform is now presented. To this end, task categories that bundle similar functionalities were identified. In particular, (i) design and evaluation of system requirements with focus on privacy concerns, (ii) specification of system and service details with focus on privacy concerns, (iii) assessment of data subject's privacy preferences, (iv) enforcement and monitoring of system's compliance with data subject's privacy preferences at run-time, (v) visualisation of analysis results, system logs, system's compliance and, finally, the generation of the PLA.

Each of these five task categories are addressed by a functional component of VPP, integrating a powerful set of tools. More specifically, the five functional components of VPP are the following:

The *Privacy Requirements Component* supports the data controller to design and process privacy requirements. This is achieved by modelling the services and the system under development from several perspectives, covering different aspects, i.e. the socio-technical environment, trust relationships between actors, security threats and business processes' compliance with privacy and security requirements.

The *Privacy Specification Component* allows the specification of further system details (by e.g., UML models), based on the requirements captured by the Privacy Requirements Component. The detailed specifications are analysed in terms of privacy and security issues, value of personal data and compliance with relevant data protection laws and regulations. This analysis is based on established privacy and security properties, such as secure information flow [17].

The *Privacy Assessment Component* allows data subjects to define their privacy preferences for data sharing and management by the data controller. Their preferences are captured by answering simple and very clear questions presented in Privacy Visualisation Component. Moreover, answers to additional questions are used for the estimation of the value of the data subject's personal data that will be presented in the PLA. The data controller uses the Privacy Assessment Component to specify these questions and also to provide required information about the processing of data subject's personal data.

The *Privacy Run-time Component* monitors data access requests and enforces data access policies. These policies for automatic enforcement are generated automatically by deriving information from system models and interpretation of data subject's privacy preferences (as described in the questionnaires). This functionality is transparent to the end users and works in the back-end. The information provided to data subjects is done through the Privacy Visualisation Component, which shows the relevant requests, issues, etc. to their data. This component is key in the integration with the system under development, as the requests have to be done through the service it offers before accessing the data.

The *Privacy Visualisation Component* acts as a unified user interface during run-time for both, data controller and data subjects, by integrating the user interfaces of the different tools of the other four components. The PLA, as the manifestation and visualisation of the system's properties and data subject's preferences, is compiled and visualised by this component.

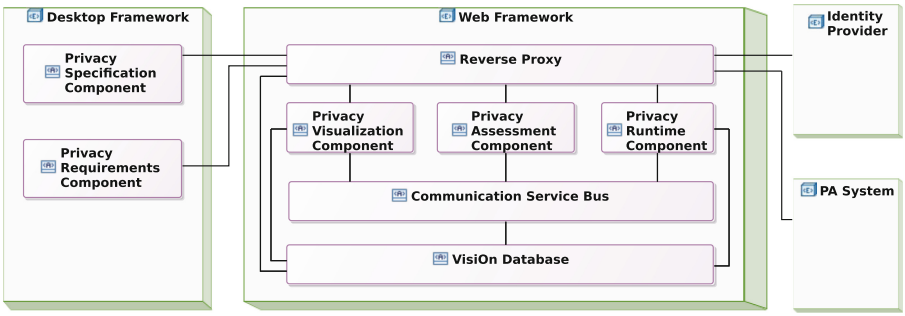

Fig. 1. VisiOn Privacy Platform: components and frameworks

Figure 1 depicts the five functional components described along with three supplemental components of VPP, responsible for connecting the functional components with each other and with external systems. These three supplemental components are left to describe.

Firstly, the *Reverse Proxy* component acts as a gateway to VPP for systems that are not part of VPP. Requests to access VPP are issued by human actors and by systems of the data controller (labelled *PA System* in Fig. 1). To avoid managing and storing sensitive account data like passwords, unauthorised access requests are redirected to an external Identity Provider, which performs users' and services' authentication. Upon successful authentication, the external Identity Provider issues a token which authorises the user or service to access VPP. Authorised access requests are passed to the appropriate internal functional component.

Secondly, the *Communication Service Bus* component integrates an Enterprise Service Bus and enables tools to directly exchange messages without persisting the exchanged information. This is used in situations where a tool has to directly react on certain events. To achieve this, the Communication Service Bus provides a message bus that supports messaging between one sender and

one receiver and messaging between one sender and arbitrary many receivers. This allows for flexibility in the communication and selection of tools. New tools can be added or replace an existing one, without requiring to modify its communication partners. A tool sending information does not need to know which tool or tools actually receive the information, a tool receiving information does not need to know which tool actually sends the information.

Thirdly, the *VisiOn Database* is a common data store, used by the functional components to persist data that may be read and processed by other components. A tool writing data to the VisiOn Database does not need to know which other tool will read this data. A tool reading data from the VisiOn Database has to know at least the location and the format of the data.

Finally, the components of VPP are integrated in two complementary frameworks, the *Desktop Framework* and the *Web Framework*. The Desktop Framework is used by the data controller's administrators only. It is used during design-time to capture and analyse the privacy characteristics, requirements and properties of their systems. It contains the modelling tools of the Privacy Requirements Component and the Privacy Specification Component. The output of the modelling tools of these components is stored in the VisiOn Database for further processing by other tools, for example for the automatic generation of questions to be answered by data subjects. In addition, the Web Framework provides run-time privacy related functionalities and also configuration settings. It has as input the data controller's privacy requirements and, based on these, data controllers can create the questionnaire with the corresponding questions. Then, the data subject can specify their privacy preferences by filling in this questionnaire. Moreover, the Web Framework displays the PLA, informing the data subjects of how their data is used, by whom and for what purpose, and also enforces the corresponding privacy policies. It is also the main interface for both data controllers and data subjects, so it is integrated with the Identity Provider of the data controller, which allows users to easily access and use the functionalities of VPP.

4 Case Study

In this section we report our experience of applying VPP to a real-world case study in the healthcare domain. This case study involves two paediatric clinics, namely Ospedale Pediatrico Bambino Gesù (OPBG) and Hospital Infantil Universitario Niño Jesús (HIUNJ) that use a telemedicine platform to exchange medical information of patients.

4.1 Motivating Scenario

The procedure of obtaining a patient's consent during medical procedure is a key aspect for guaranteeing transparency in the treatment of personal healthcare data. For this reason, the consent form includes a written detailed document which patients should carefully read before signing. This process is due even when

a patient seeks urgent healthcare, unless immediate medical treatment must be provided in order to prevent potential death or complications. Through the consent form, health professionals establish a formal relationship with patients or their legal guardian, who provides all the necessary information that facilitates the decision making on both medical and personal data processing.

The information included in the consent form is complementary to and should not substitute the information provided orally by the health personnel during a treatment. Moreover, the written consent form is part of the medical record. In particular, the responsibility of filling a medical record is bound by certain rules. Consent to medical and surgical treatment is personal and can be provided only by the patient. In case the patient is unable to give a consent, medical data and approval of informed consent is respectively provided by the person exercising parental responsibility or by a legal guardian. The exercise of parental or tutorial responsibility is implemented on the declaration. Note that consent cannot be delegated, so the person who legally represent the minor is the only one entitled to provide consent to medical treatment. Another mandatory condition is the state of necessity. If the patient is in a state of emergency, the physician can act without the acquisition of the consent form because of the need to save the patient from the danger of serious harm or a life threat.

In this scenario, a platform, such as VPP, that allows the patient to fully control their information through permitted and prohibited operations and consents is a massive breakthrough. Furthermore, VPP increases awareness and understanding of the importance of protecting their data, highlighting the benefits/risks of signing/not signing a consent form. These requirements are the most important but there is a full list of high level requirements to consider in the process of compiling an aware consent form for a telemedicine scenario. The patients should have a clearer picture of the benefits/risks for compiling it.

The processes in telemedicine services fall within the sensitive data being processed by electronic instruments, which are currently regulated by the provisions of Directive 2002/58/EC [2]. The methods and the solutions necessary to ensure confidentiality, integrity and availability of data should therefore be adopted in accordance with the security measures explicitly provided in the Directive 95/46/EC [1], covered under the GDPR [5] and the new regulation replacing the Directive 2002/58/EC [2], which can be found in [3].

The provision of a medical performance is historically connected to the physical presence of the patient in a hospital doctor's studio or of the doctor in the home of the patient. The eHealth services try to change this traditional approach. The new technology could help doctors to provide some medical performances by remote place. The major problem of medical services is related to the type of data exchanged. In each medical service, data is classified as sensitive data and this kind of data request a high level of protection of the three aspects of security (Confidentiality, Integrity and Availability) [16].

An important aspect of the eHealth is that the clinical record (totally or partially) has to move from one site to another. Consequently, this transfer aims

to raise two important issues. First, who has the right to access this data and secondly, if the patient has given their consent to transmit their data.

Another important problem is related to how the patient's sensitive data is transmitted. In eHealth, data is transmitted by video, audio and files. For this type of data it is necessary to develop modular system that includes technical and/or organisational enforcement measures, able to balance the right to protect the sensitive data and the processing of this data necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent [5].

4.2 Privacy Level Agreement for Hospitals

Patients, through Privacy Visualisation Component and Privacy Assessment Component of VPP, are able to define the privacy preferences concerning their data, defining what data they wish to share and how they expected to be managed. The questionnaire is a user-friendly way of defining the preferences, using natural language more simple and easy to understand by the patients. For the generation of PLAs that will capture the privacy preferences of the patients, the questionnaire provided by the Hospital and the answers given by the patients are required. In particular, the data processor accesses the Privacy Assessment Component, which guides them to create questions to the patients about the Hospital System and how they wish their data to be managed. Moreover, this component is responsible for collecting the relevant information that has been generated in the Privacy Requirements Component, regarding the access rights that are documented for each piece of data transmitted within the Hospital system. Thus, the data processor forms questions accordingly, responsible for capturing patients' preferences regarding these access rights. An instance of this questionnaire is depicted in Fig. 2.

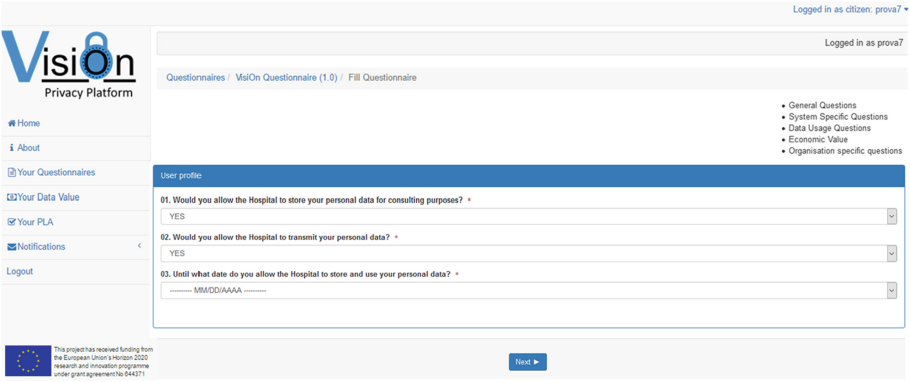

Fig. 2. A questionnaire for an eHealth service

After the development of the questionnaire, the data processor evaluates the sensitivity of the data mentioned in the questions. These values are inserted

through the Privacy Specification Component and then, they are depicted in a web diagram form in the PLA. This diagram contains the value from the data processor perspective, the patient's perspective, and the average of the values of all the previously registered to the eHealth service patients. Next, the data processor is ready to publish the questionnaire where the patients can answer, providing also their values for the sensitivity of their data. For each patient's answer, the Privacy Visualisation Component collects the responses, the relevant laws, the information derived from the modelling of privacy information, which includes the security and trust analysis results and the data value of patients' data, and finally, composes the PLA. A PLA, as it is depicted in Fig. 3, describes a patient's personal privacy preferences, along with statistics, policies and laws applied by the hospitals. The structure and the design of the PLA is simple enough and easily understandable by each patient, including textual and visual information. This information is up-do-date, so patients can always find all their information compiled in a single place. This functionality is very useful as it provides a complete description of patients' privacy status.

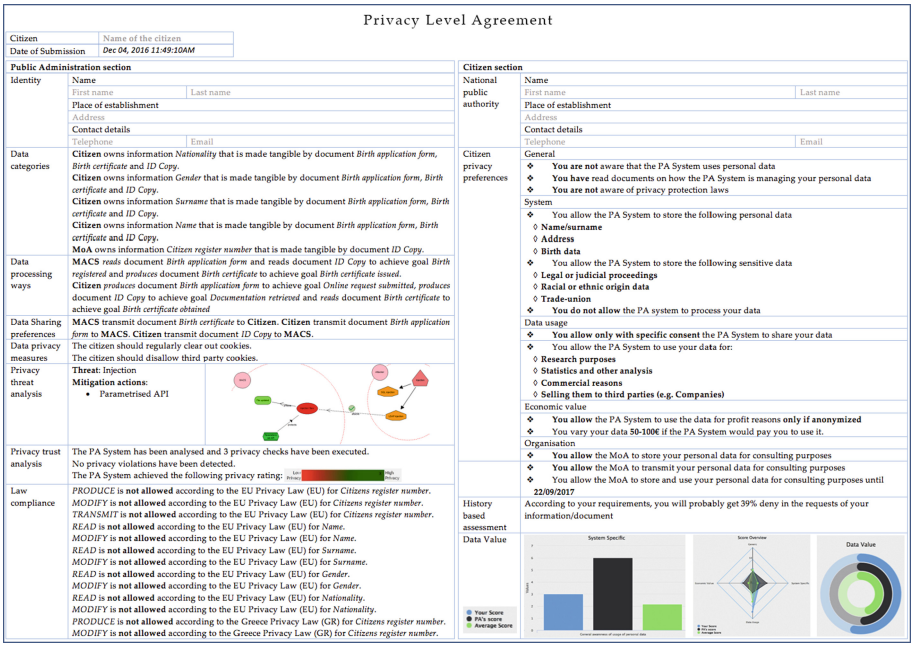

Fig. 3. A patient's PLA

4.3 Applying VPP in eHealth

Before deploying VPP at the premises of OPBG and HIUNJ, the physicians at each hospital were able to retrieve patient data from the hosting hospital's

repository and send it through a telemedicine application, without any restriction. The application was extended by including the functionality of sending a request to VPP before querying to the repository of documents of patients. The aforementioned request contains information about the person or institution that asks for the health data, the identification of the patient concerned and the items that can be susceptible of privacy protection. VPP compares the fields in the request to the privacy preferences that are recorded in that moment.

There are two important points to be taken into account. First, before any data is required by the doctors, the parents or tutors of the minor should fill a questionnaire presented to them by VPP. That questionnaire is stored in the VisiOn Database and can be modified any time the parents/guardians wish to. Second, both hospitals must deploy an instance of VPP to protect the data stored in their premises. The parents/guardians must fill a questionnaire in each hospital in which data of their child is stored. As an example, if an Italian child on holidays in Spain goes to HIUNJ and the doctors there think they must see a report or a x-ray image created and stored in OPBG, supposing they have access to the corresponding application there (e.g., OBGclinico), the parents must have filled the questionnaire of VPP in OPBG before.

To monitor the application of rules for privacy protection, VPP is tested in three simulated scenarios. In the first scenario, a patient has a complex and rare disease and the medical staff in charge of their follow-up decide to ask a teleconsultation to a specialist group in another hospital in order to decide the most appropriate diagnostic procedures and therapy. The physicians at OPBG make a diagnosis, producing a medical report and some medical images, while the specialised group at HIUNJ retrieves these files from an OPBG web application and confirms whether the diagnosis is correct or not. In the second scenario, a patient has a chronic disease and is followed up by OPBG. While the patient is travelling abroad, presents symptoms of their disease and visits HIUNJ. Then, the physician in HIUNJ needs to perform a televisit with the patient's physician at OPBG. The first retrieves the patient clinical history and some data from OPBG system to perform a more accurate diagnosis. In the third scenario, a patient with a rare disease moves to another European country with their family and needs to transfer their clinical dataset, in order to allow the hospital in the new location follow them up appropriately.

These scenarios have been executed with patient data partially produced for the purposes of our project and do not belong to any real patient. This data is combined with a composition of real clinical data taken anonymously and retrospectively from real patients, to preserve anonymity while remaining realistic. A hospital eHealth application hosts the patient's clinical history, a computer tomography image, a histological and a surgical intervention report.

In this use case, technicians (hospitals personnel) are in charge of modelling the overall system and setting the infrastructure. Doctors (hospitals personnel) connect to a web application from another hospital to access the health data of a patient and parents (or tutors) of a patient that connect to VPP, to declare permissions to let the doctors of another EU country to access or not the health data of their child. For evaluating VPP, two trials were performed. In the first

trial, the objectives and the functionalities of the VPP were explained to the parents/tutors of the patients. Next, the parents/tutors filled a consent form to authorise the use of their answers for the purpose of this case study. After their interaction with the VPP, i.e. after they fill the questionnaire related to their privacy preferences, and the creation of the PLA for each patient/tutor, they answered a questionnaire[8] in order to assess the usability and usefulness of VPP. In the second trial, the IT personnel was trained on how to use the Desktop Framework tools and how to create a questionnaire related to the e-Health service. Next, they were provided a questionnaire(see Footnote 8) similar to the one the parents/tutors, in order to evaluate VPP from the data processor's perspective.

The data processors, after the VPP installation and the integration with the hospital infrastructure, are able to model their systems and elicit privacy requirements, by using the Desktop Framework of VPP. After the data processors create a questionnaire on the VPP web portal, they attach the metadata for each question (metadata is basically keywords to add during the questionnaire building procedure). Then, when a patient registers on the eHealth service and compiles the questionnaire, this metadata are stored on the VPP back-end, according to the answers given. The models developed by the data processors are also stored on the VisiOn Database. The patients, after answering the questionnaire, can visualise their own PLAs and the attempts to access their resources, checking the notifications created by the Privacy Runtime Component. The data processors are also able to monitor these processes, for each patient, according to the level of authorisation that the organisation granted them for this information. When a physician from another hospital tries to retrieve the data from the web application integrated with the Web Framework of VPP, they receive feedback from VPP, according to the PLAs set up by the patients.

In a manner wholly transparent for users, the requests made by the clinicians to get the desired documents are converted to a XACML format, which is semantically very rich. These transformed requests are immediately sent to VPP that decodes and checks them against the policies derived from the preferences recorded by the patient, or the parents, or legal tutors of the patient. With the response of a simple PERMIT or DENY statement, the developed application proceeds to request data to the databases in the servers of the health system, or notifies the doctor that the data required cannot and should not be granted, because the patient does not wish so.

The contingency of an emergency or danger of death situation has been taken into account. The possibility that the doctor asserts that a situation of that extreme sort is taking place in the moment of the consultation has been added to the interface of the request of the data. In that sense, the permissions of data to be transmitted in case of scientific studies or actual consultations for second opinions are also added in the questionnaires, and also, the corresponding indications in the application for the doctors to input at the time of the requesting.

[8] This questionnaire is not part of VPP and has been created only for the purposes of the trials and the evaluation of the platform.

4.4 Discussion

One of the key aspects to consider in the future development of ICT hospitals' services is the EHR. Though not universal, EHR allows the digital management of health information and medical procedures, including telemedicine. Currently, interoperability between different EHR platforms has raised significant issues [20]. Moreover, the development of further specialised digital services may require some efforts to guarantee transparency of telemedicine transactions between hospitals and also, between patients and hospitals. An ideal EHR should contain, in the first place, the informed consent properly filled out, a copy of the resignation letter which must be completed even in case of patient death, and the hospital discharge form, which must be filled up through the IT application, which should be in compliance with national and regional regulations. All results of the provided services, including telemedicine, remote monitoring and specialist consultations, all therapies prescribed and administered, internal/external transfers of the patient within the different hospital's operating units and integrated graphics of hospital stay and of intensive areas must be recorded. Furthermore, medical assessments pre-sedation, pre-anaesthetic, pre-surgery (in cases where such procedures are foreseen) and surgical procedures performed shall be documented in the electronic surgical register, and a copy of the surgical report should be attached to the health record.

The VPP trial in the hospitals had involved the telemedicine and teleconsulting services but this kind of eHealth services are only a limited range of electronics' medical services. The evolution of the technical aspect of VPP will follow three major roads. The first is to expand the enforcement on the only exchange of EHR documents to the medical information exchanged orally and with video in telemedicine and teleconsultation; the second is to cover other eHealth services, such as consultation of EHR by the internal staff of the hospitals and by the patient himself or to all those electronic medical devices; the last way is to expand the enforcement to devices not specifically medical but which contain information comparable to sensitive data (e.g., smartwatch, fit band/fitness tracker, smartphone, etc.). The data subjects upon their registration receive their credentials and after answering a questionnaire, a PLA is generated for each organisation, which could be problematic as services adopt VPP. To tackle this problem we foresee the use of common credentials for every service, e.g., the social security number. However, regarding the multiple PLAs, we will investigate how to improve *PLA portability* between different installations of VPPs.

The main issue related to the integration of VPP with EHR lies in the fact that there is no standardised approach in Europe in the development of EHRs. For example, the situation of the Italian EHR is managed at regional level and the situation is fragmented [6]. European health organisations at all levels should be able to provide online services, i.e. teleconsultation, e-prescription, e-referral, telemonitoring and telecare, but these are not mutually compatible. These services are expected to increase accessibility to healthcare, appropriateness and quality of care, and decrease direct and indirect costs associated with care.

5 Conclusions

This paper presents a platform-supported approach for privacy management of citizens' data regarding its management and use. Data subjects can then safely share their data with organisations in order to take advantage of the e-services they provide. The agreement between data controllers and subjects regarding the use of data is conceptualised in a PLA, which is elicited through clear and non-technical questionnaires. This allows PAs, using our approach, to increase transparency and trust in their services.

From social perspective, VPP aims to raise data subjects' awareness regarding the value of their data through enhanced visualisation elements, and information that can be exploited of the determination of data subjects' privacy preferences. This way, and as previously explained, transparency and trust will increase the number of users using e-services. Data controllers can benefit from VPP, since they can manage personal data in an accountable and transparent way, and also provide data subjects with the option of controlling their privacy settings, regarding personal data they are obliged to share. Monitoring how personal data is used after it has been provided to data controllers is one of the main functionalities of VPP, provided by the Web Framework, making VPP play a critical role in the maximisation of transparency and accountability regarding activities of data controllers related to data subjects' personal data.

From technical perspective, VPP integrates a set of software engineering methodologies and tools across different levels, from the elicitation of users' privacy requirements to the enforcement of privacy policies during run-time, and different perspectives, from data evaluation to privacy assurance. Such integration provides a clear advantage over existing software engineering approaches and tools, since it enables a holistic analysis of both data controllers and data subjects' privacy preferences. To the best of our knowledge, VPP is the only approach in the literature that is able to identify and analyse privacy and security threats of data controllers' IT systems and to also allow data subject to declare their privacy preferences.

VPP represents a useful tool that can support the verification of data controllers' compliance with the GDPR. Future work includes the enhancement of tools for policies and law compliance, in order to allow data controllers to check their compliance with the GDPR and also, how to implement it in their systems. This will have a big impact on data controllers as, in this way, they will be able not only to provide privacy enforcement for the data subjects, but also they can use VPP for making them adhere to the GDPR, ensuring data subjects that their data is protected, according policies at organisational, country or European level. Finally, even this work focuses on requirements stemming from GDPR, approach or parts of it are applicable to systems and services under different legislation.

Further development of VPP can lead to mobile applications that data subjects can use to check and define their privacy preferences, access to statistics on the use of their data, notifications, etc. As the market of mobile applications is growing by year, our approach would be the best complement for the cloud

environment and will facilitate data subjects in controlling their data and data controllers in improving their transparency. VPP integration in EHR, such as the SMART[9], which focuses on and supports the development of mobile apps integrated with EHR systems, is also part of possible future work.

Finally, another future work of VPP concerns the Industrial Data Space [21], which is a virtual data space for the secure exchange of data in business ecosystems, for creating and using smart services and innovative business processes, while at the same time ensuring digital sovereignty of data owners. The Medical Data Space is a domain-specific instantiation in the Medical Domain to address the particular challenges and requirements that arise in this domain. To address the data privacy concerns in this context, results and tools from VPP are going to be used. For example, the Industrial Data Space will offer privacy-relevant data analysis services, including an anonymisation service, where the tools and techniques on model-based privacy and security analysis from VPP will be used to determine that the desired level of privacy has been reached.

Acknowledgement. This research was supported by the Visual Privacy Management in User Centric Open Environments (VisiOn) project, supported by the EU Horizon 2020 programme, Grant Agreement No. 653642.

References

1. European commission: Directive 95/46/ec of the european parliament and of the council. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046. Accessed 14 Jun 2017
2. European commission: Directive 2002/58/ec of the European parliament and of the council, July 2002. http://ec.europa.eu/justice/data-protection/law/files/recast_20091219_en.pdf. Accessed 14 Jun 2017
3. European commission: Proposal for a regulation of the european parliament and of the council, January 2012. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011. Accessed 14 Jun 2017
4. European commission: Eurobarometer 431 - data protection report. Technical report (2015)
5. European parliament: Regulation (eu) 2016/679 of the european parliament and of the coucil 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) (2016). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en. Accessed 14 Jun 2017
6. Forum-pa - osservatori digital innovation del politecnico di milano: Che cos'è il fascicolo sanitario elettronico e come utilizzarlo, December 2016
7. Colombo, P., Ferrari, E.: Towards a modeling and analysis framework for privacy-aware systems. In: 2012 International Conference on Privacy, Security, Risk and Trust (PASSAT), and 2012 International Conference on Social Computing (SocialCom), pp. 81–90. IEEE (2012)

[9] https://smarthealthit.org/an-app-platform-for-healthcare/about/.

8. CSA: Privacy level agreement outline for the sale of cloud services in the European Union. Technical report, Cloud Security Alliance, Privacy Level Agreement Working Group, February 2013
9. DErrico, M., Pearson, S.: Towards a formalised representation for the technical enforcement of privacy level agreements. In: 2015 IEEE International Conference on Cloud Engineering (IC2E), pp. 422–427. IEEE (2015)
10. Drogkaris, P., Gritzalis, S., Lambrinoudakis, C.: Employing privacy policies and preferences in modern e-government environments. Int. J. Electr. Governance **6**(2), 101–116 (2013)
11. Earp, J., Anton, A., Jarvinen, O.: A social, technical, and legal framework for privacy management and policies. In: AMCIS 2002 Proceedings, p. 89 (2002)
12. Ebrahim, Z., Irani, Z.: e-Government adoption: architecture and barriers. Bus. Process Manage. J. **11**(5), 589–611 (2005)
13. Farzandipour, M., Sadoughi, F., Ahmadi, M., Karimi, I.: Security requirements and solutions in electronic health records: lessons learned from a comparative study. J. Med. Syst. **34**(4), 629–642 (2010)
14. Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O., Toval, A.: Security and privacy in electronic health records: a systematic literature review. J. Biomed. Inform. **46**(3), 541–562 (2013)
15. Greenhalgh, T., Hinder, S., Stramer, K., Bratan, T., Russell, J.: Adoption, non-adoption, and abandonment of a personal electronic health record: case study of healthspace. BMJ **341**, c5814 (2010)
16. ISO/IEC: 27000:2016 information technology - security techniques - information security management systems - overview and vocabulary. Technical report (2016)
17. Jürjens, J.: Secure information flow for concurrent processes. In: Palamidessi, C. (ed.) CONCUR 2000. LNCS, vol. 1877, pp. 395–409. Springer, Heidelberg (2000). doi:10.1007/3-540-44618-4_29
18. Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: the PriS method. Requirements Eng. **13**(3), 241–255 (2008)
19. Li, J.S., Zhou, T.S., Chu, J., Araki, K., Yoshihara, H.: Design and development of an international clinical data exchange system: the international layer function of the dolphin project. J. Am. Med. Inform. Assoc. **18**(5), 683–689 (2011)
20. Mahfuth, A., Dhillon, J.S., Drus, S.M.: A systematic review on data security and patient privacy issues in electronic medical records. J. Theoret. Appl. Inform. Technol. **90**(2), 106 (2016)
21. Otto, B., Auer, S., Cirullies, J., Jürjens, J., Menz, N., Schon, J., Wenzel, S.: Industrial data space: digital souvereignity over data. Technical report, Technical Report, Fraunhofer-Gesellschaft (2016)
22. Rezaeibagha, F., Win, K.T., Susilo, W.: A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Inform. Manage. J. **44**(3), 23–38 (2015)
23. Spiekermann, S., Cranor, L.F.: Engineering privacy. IEEE Trans. Software Eng. **35**(1), 67–82 (2009)
24. (W3C), W.W.W.C.: Platform for privacy preferences (p3p) project (2016). https://www.w3.org/TR/P3P11/. Accessed 14 Jun 2017