Visual Privacy Management in User Centric Open Environments

Vasiliki Diamantopoulou, Michalis Pavlidis

School of Computing, Engineering and Mathematics,
University of Brighton, Brighton, UK
{v.diamantopoulou, m.pavlidis}@brighton.ac.uk

***Abstract*—In open and dynamic online services the exchange of information is demanded to be easy, simple and always available. However, potential users of online services are still reluctant to outsource sensitive data to these services, mainly due to lack of control over management and privacy issues of their data. This becomes more complex when dealing with Public Administrations (PAs) which handle data of citizens, where the latter are obliged, in many cases by law, to do so. This paper presents the VisiOn Privacy Platform, which analyses privacy preferences, and introduces the concept of the Privacy Level Agreement, capturing the PAs and citizens privacy requirements, thus supporting transparency and accountability for PAs.**

***Keywords*—Privacy Management, Privacy Level Agreement, Public Administration.**

I. Introduction

Privacy is considered as an increasingly important concern in the domain of Information and Communication Technologies (ICT), attracting much attention recently [1], [2]. With more and more sensitive and confidential information stored, shared and manipulated at digital level [3], individuals and organisations expect appropriate measures to ensure privacy of such information. Recent research indicates that the protection of users' privacy has become crucial for organisations in order to maintain a high standard of services and retain competitive advantage [4]. Moreover, the new EU directive [5] on data privacy forces organisations to manage data in a specific way with regards to privacy. In this sense, it is pivotal that organisations' information systems are developed and operate in a way that improve transparency of citizen data sharing. Towards this direction, we have developed a novel platform that enables privacy analysis for citizens and PAs e-services. The VisiOn Privacy Platform aims to increase citizen confidence in the PAs e-services, allowing them to set their privacy needs/preferences, stimulating them to consider privacy and data protection in a proactive manner. Additionally, the platform contributes to the increase of transparency and accountability of PAs, with regards to processing and sharing citizens personal and sensitive information, without revealing it to parties not authorised/approved by the citizen, thus enhancing citizens trust. Finally, VisiOn Privacy Platform supports a way for a clear visualisation of privacy preferences and some insights of the value of data managed, supporting citizens' decision making with regards whether data should be shared.

II. Research Challenges

For the development of the VisiOn Privacy Platform we had to deal with a number of research challenges. It is important for the PAs to be able to clearly specify citizen privacy needs, provide them with feedback on how their data is shared and whether sharing of their data conflicts with their needs. On the other hand, PAs should enable citizens to understand the potential threats and vulnerabilities to their privacy needs, as well as trust relationships that might endanger their privacy.

We address the above challenges by proposing the use of the Privacy Level Agreement (PLA), since it supports a mutual agreement between a citizen and a PA, regarding the citizen's privacy needs and the transparency of citizens' data sharing. On the PAs side, the PLA can contribute to the achievement of the desired degree of their transparency, increasing the awareness of citizens concerning the preservation of their personal data and allowing them to set their preferences about the handling of their data. On the citizens side, they can be informed about the usage of their data and how it is managed by any organisation. Moreover, they are notified or they are aware when someone requests access to their data, they know if and when an organisation wants to share their data with third parties, and finally they are able to know whether the organisation respects the privacy legislation, at national and European level.

III. The Platform

The VisiOn Privacy Platform is designed to support both PAs and citizens. The PAs use the platform to capture privacy requirements and compose questionnaires for citizens, in order the PLA of each citizen to be created. Citizens use the platform to specify their privacy preferences. The platform, depicted in Fig. 1, consists of five components, each one is responsible for specific procedures. The *Privacy Requirements Component* is responsible for the modelling and consistency analysis of citizens privacy requirements and business processes, the compliance, and the threat and trust analysis on the PA privacy needs and requirements. The *Privacy Assessment Component* elicitates citizens' privacy requirements through formulated

978-1-5090-5476-3/17/$31.00

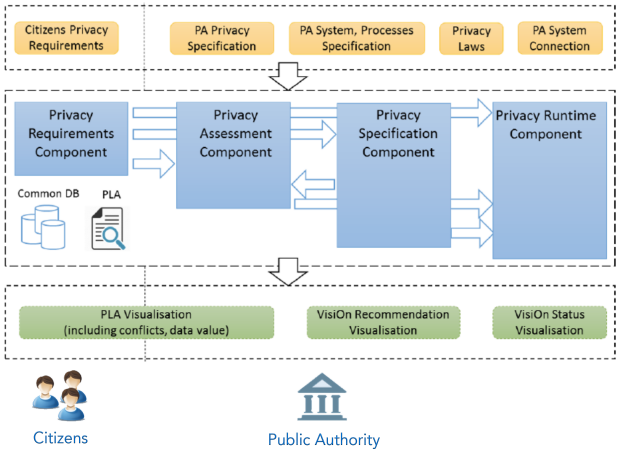

Fig. 1. The VisiOn Privacy Platform Architecture

questions, enriched with metadata for automatic processing of questions and answers. The *Privacy Specification Component* specifies the PLA with security and privacy reports, showing the compliance with EU privacy laws and increasing awareness on data valuation. The *Privacy Runtime Component* monitors events and traffic, and evaluates the requests based on privacy preferences, ensuring the control on the access to data. The *Privacy Visualisation Component* provides user interface to citizens and to PAs.

IV. Description of Pilots

The evaluation of the platform is based on scenarios focused on the communication of citizens with governmental departments and with hospitals, covering real-life conditions. They include three different pilot scenarios across two different scenario types, i.e. PA and citizen and PA with cross-border PA, involving four PAs from three European countries, namely an Italian Ministry and a local PA in Greece for the first type and healthcare PAs across borders of Italy and Spain, for the second type. The first scenario type consists of two cases; the first case concerns Italian companies that are obliged to provide their financial data in order to take advantage of the tax relief that the respective Ministry offers. It is of utmost importance to protect any transferred data since they constitute valuable asset of each company. In the second case, a Greek citizen is asked to provide their personal data in order to acquire an official document by the corresponding Municipality. The protection of the citizens' personal data is the main concern. The second scenario type is about the transmission of medical data of children from an Italian hospital to a Spanish one. This scenario type consists of three cases; i) a patient that needs a teleconsultation to a specialist group in another hospital, ii) a patient with chronic disease needs to perform a televisit with a doctor of the medical staff in charge of them while travelling, and iii) a paediatric patient with a rare disease that moves to another EU country with their family and needs to transfer their medical data. This scenario type covers three interesting aspects. The first one is the transmission of data from one country to another, the second one is that the owners of the data are children, and the third one is that the data contain sensitive medical information. In this case, the preservation of privacy is of utmost importance and consequently we will have the opportunity to evaluate how the VPP can contribute to this dimension.

V. Validation

The VisiOn Privacy Platform will be validated in real-life conditions. The validation will be performed by pilot experts by defining the specific scenarios and validation cycles. Validation within context, organisational environment and conditions that reflect reality to the best possible extent, will involve individual participants and simulated or their real personal data. The various project stakeholders, i.e. technical experts and end-users (i.e. citizens and patients) will assess the performance of the platform and test its various outputs.

Validation begins with an execution of a pre-round of tests by the end-users, in order to verify the platform's successful integration into the PAs pilot systems/services and infrastructures. Thereafter, the two pilot trial cycles will be executed. The first one will focus on the evaluation on the functionalities of the platform. It will be conducted by employees with administrative and technical skills in order to provide feedback, leading to the improvement of the platform. The second pilot trial will test the final version of the platform; end users will be asked on their perception of the platform and the level of confidence inspired, on how the PAs handle their data.

VI. Conclusion

PAs should realise the importance of the adoption of a privacy culture that enhances their trustworthiness by making their systems and procedures more transparent. Towards this goal, the VisiOn platform, through the delivery of the PLA, will ensure the awareness of citizens about the use of their personal data, and that their privacy preferences are respected.

Acknowledgement

This research is supported by the EU H2020 Research and Innovation programme under G.A. No. 653642, project VisiOn (Visual Privacy Management in User Centric Open Environments).

References

[1] L. Rainie, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish, "Anonymity, privacy, and security online," *Pew Research Center*, vol. 5, 2013.

[2] E. Commission, "Eurobarometer 431 - data protection report," Tech. Rep., 2015.

[3] G. T. Duncan, R. W. Pearson *et al.*, "Enhancing access to microdata while protecting confidentiality: Prospects for the future," *Statistical Science*, vol. 6, no. 3, pp. 219–232, 1991.

[4] PwC, "Moving forward with cybersecurity and privacy - how organizations are adopting innovative safeguards to manage threats and achieve competitive advantages in a digital era," Key findings from The Global State of Information Security Survey 2017, Tech. Rep., 2017.

[5] E. Parliament. (2016) 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).