Privacy Level Agreements for Public Administration Information Systems

Vasiliki Diamantopoulou, Michalis Pavlidis, and Haralambos Mouratidis

School of Computing, Engineering and Mathematics
University of Brighton
{v.diamantopoulou, m.pavlidis, h.mouratidis}@brighton.ac.uk
http://www.sense-brighton.eu/

Abstract. Improving Public Administration (PA) operations and services is a major focus globally; they should be transparent, accountable and provide services that improve citizens' confidence and trust. In this context, it is important that PAs have the ability to define agreements between citizens and PAs and that such agreements can be used in the context of PAs Information Systems to specify citizens' privacy needs, provide feedback on data sharing and enable PA departments to analyse privacy threats and vulnerabilities, compliance with laws and regulations and analyse trust relationships. We propose the use of the concept of Privacy Level Agreement (PLA) to address the aforementioned issues. The PLA is formally specified, based on an XML schema, which enables its automated use.

Keywords: Privacy Level Agreement, Privacy Management, Citizen, Public Administration

1 Introduction

Advancements in ICT have enabled Public Administration (PA) to offer an increasing number of e-services to citizens [2]. The benefits provided to citizens, such as increase in efficiency, productivity, and growth [7], can be significantly improved when information is shared across multiple information systems belonging to different PAs (one-stop concept [15,13]) and when citizens do not need to input the same information across different PA information systems.

On the other hand, a recent EC initiative for capturing European citizens' opinion concerning their attitude to data protection [3] revealed that 69% are concerned that the personal data they provide may be used for a purpose other than that for which it was collected. Moreover, the General Data Protection Regulation (GDPR) [12] on data privacy forces organisations to manage data in a specific way with regards to privacy. In such context, it is crucial that PA information systems are developed and operate in a way that improve transparency of citizen data sharing. In doing so, it is important that PAs are able to clearly specify citizen privacy needs, provide them with feedback on how their data is shared and on whether sharing of their data conflicts with their needs. In addition, PAs

should enable citizens to understand potential threats and vulnerabilities to their privacy needs, as well as trust relationships that might endanger their privacy. We address this challenge by proposing the use of the concept of Privacy Level Agreement (PLA), which formalises a mutual agreement between a citizen and a PA regarding the citizens privacy needs and supports the transparency of citizens' data sharing. The PLA is delivered in a form of a structured agreement that consists of fields, each of them capturing important and obligatory information with regards to privacy of citizens' data. We also propose an XML schema to enable the creation and management of machine-readable PLAs, allowing its utilisation by distributed information systems, thus addressing interoperability issues.

The paper is structured as follows: Section 2 discusses related work while Section 3 presents the context and the definition of the PLA and also provides the specification of it. In Section 4 we provide the outcome of this work and finally, Section 5 summarises the paper.

2 Related Work

The concept of PLA has been launched as an initiative to capture privacy aspects of cloud providers. The Privacy Level Agreement Working Group of the Cloud Security Alliance has defined a PLA in the context of cloud services [4]. Similarly, the concept of PLA has been presented by [5] as a standardised way for cloud providers to describe their data protection practices. In this environment the PLA is considered as a means for the cloud providers to ensure that their privacy policy is communicated to the service consumers. However, these works are limited only to privacy aspects of cloud provision and do not provide support for specification of user preferences and needs or ways to define privacy threats and vulnerabilities related to these needs.

On the other hand, the literature provides many examples of works that focus on the specification of Service Level Agreements (SLAs) which refer to the mutual agreement that ensures the obligations and the requirements both of a service provider and a customer (e.g., [1,9]). In contrast to PLA, an SLA does not take into account privacy aspects of the agreement between a service provider and a service consumer.

Concerning the privacy policies enforcement, the idea of a standardised way for web sites to communicate with users about their privacy policies in a standard machine-readable format has been introduced by the Platform of Privacy Preferences (P3P) project [16]. This standard enables web browsers and other user agents to interpret privacy policies on behalf of their users, assisting them to decide when to exchange data with web sites. However, P3P was designed for static environments where users privacy preferences are not expected to change and it also provides limited support for specification of privacy threats and vulnerabilities that might endanger the privacy needs. Finally, in [6] the authors propose an architecture that promotes the employment of privacy policies and preferences. They introduce the Privacy Controller Agent for storing and com-

paring service providers' privacy policies and user privacy preferences. However, this work does not provide an agreement between the interested entities but rather an architecture to define privacy policies.

3 Specification of a Privacy Level Agreement

In the context of our work we define a PLA as the mutual agreement of the privacy settings between a service provider (i.e. Public Administration (PA)) and a user (i.e. citizen), where the former will commit to provide and maintain these settings throughout the provision of the service. Thus, the PAs can (i) handle the personal data they keep taking into account citizens' privacy needs, (ii) provide information concerning the processes they follow and the management of personal data and (iii) demonstrate that they have proceeded to all the necessary actions to make their systems robust, mitigating all possible threats.

The structure of the proposed PLA is depicted in Fig. 1 as a UML class diagram which shows the concepts of the PLA, their hierarchy, and their relationships with each other. The PLA is represented as a class that contains two subclasses, the first with information related to the PA and the second with information related to the citizen. In turn, each section contains a number of fields that includes information related to the privacy of the citizens' data.

3.1 Public Administration PLA Section

The PA section has the following fields. For each field we provide a short description and we specify them using an xml schema[1]. The schema enables us to represent the PLA with the potential to be machine readable and to allow information systems to further process the information included in the PLA, for example, for enforcing privacy polices.

Identity: This field describes the publication of administration's name, place of establishment, and the contact details of the PA's data controller administrator. Assigning such a responsibility to an employee of the organisation is important so that the citizen has a point of contact in case they want to make a query, contributing to the accountability of the service [10].

Data: Specifies which personal data the citizen needs to provide to the PA.

Data processing rights: Provides information about processing and storing of citizens' data. Acquiring complete information about processing and storing of their personal data to the PAs' information systems, citizens are fully informed, e.g., on the location of their stored data, on the processing rights, etc.

Data Sharing Preferences: Provides information about third parties that can have access to citizens' data, since as the PA has the ability to collect huge amount of citizen data, this may attract external parties that want to acquire the data [10].

[1] `http://www.sense-brighton.eu/xml_pla/`

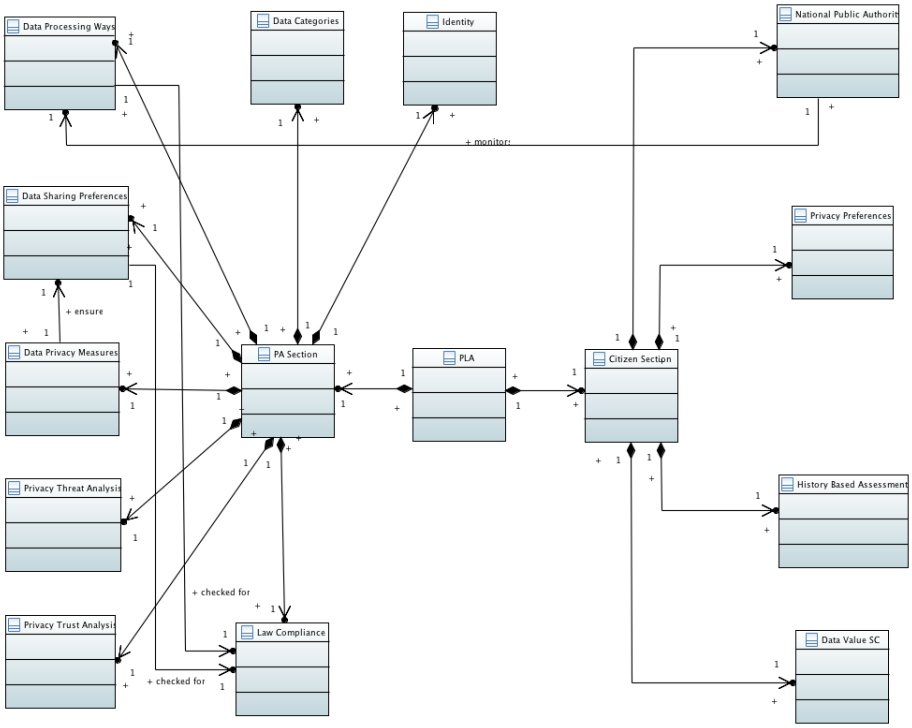

Fig. 1. PLA stucture

Data Privacy Measures: Specifies the technical, physical and organisational measures in place to protect citizens' personal data against accidental or unlawful destruction or loss, alteration, unauthorised use, modification, disclosure of access, and against all other unlawful forms of processing. These measures can ensure the satisfaction of the relevant privacy requirements.

Privacy Threat Analysis: Provides the threat analysis of the PA's privacy needs and requirements. Citizens need assurances that the PA introduces appropriate mechanisms and processes to support the privacy needs, and inform them when these needs are not followed due to either PA policies or legislation. Having such information improves the transparency of PA's operations in terms of data management, and it therefore helps to improve citizens' trust.

Privacy Trust Analysis: Provides the trust analysis of the PA's privacy needs and requirements. Since trust is considered a very important factor for the adoption of e-government services [14], PA's have to demonstrate that the infrastructure and the staff responsible for the operation of the infrastructure can be trusted [8,11].

Law compliance: Provides information on whether privacy requirements are complaint with privacy laws at a national and EU level. In particular, it specifies the constraints imposed by regulations and laws and also how the PA uses/man-

ages citizen data. Also, it verifies if the data management specified by the PAs respects the constraints specified in laws and regulations.

3.2 Citizen PLA Section

The citizen section has the following fields:

National Public Authority: Contains the details of the National Public Authority responsible for protecting citizens' personal data rights. Adding such information to the PLA will raise the awareness of the citizens about the protection of their data rights by the specific national public authority.

Citizen Privacy Preferences: Contains the privacy preferences of the citizen that have been collected by the PA. The study of [17] reveals that the government applications that engage citizens and allow interactivity with them, have positive payoffs for trust in government.

History based assessment: Consists of an analysis of the citizens' privacy preferences and the generation of a prediction of the possible outcomes of subsequent requests. It contains an estimation of the accepted or denied requests for citizens data, based on their requirements available and the aggregated statistics about other citizens, collected up to that moment.

Data Value: Contains the citizens' perspective concerning their data and the valuation of citizens' data by the PA and the average valuation of all the citizens. This information can increase transparency since it communicates to the citizen the relative value of data and consequently, it will increase the trust of the citizen in the PA.

4 Illustrative example of a Privacy Level Agreement

To better demonstrate the applicability of the PLA in the context of a PA information system, we apply the defined PLA to a real-case study. In this scenario, a local Public Administration, the Municipality of Athens (MoA), makes use of their information system MACS (Municipality Athens Citizen System) to provide e-services to Athenian citizens and to store all their data. Although multiple services are provided through MACS, in this paper, due to space limitations, we focus on the e-service related to the issue of a birth certificate. As part of that service, the PA supports the creation and enforcement of a PLA. In doing so, the PA requests that all citizens requiring the birth certificate e-service are provided with the option to provide their privacy preferences and create a PLA. The interaction among the citizen and the PA is depicted in Fig. 2 and described as follows. A citizen requests the issue of a birth certificate, using the MACS system. The MACS receives the request and presents a questionnaire that enables the citizen to declare their privacy preferences. Based on the citizen's answers, the PA information system proceeds to the creation of the PLA which is presented to the citizen. After the citizen has received their personalised PLA, they are requested by the MACS to give all the necessary data for requesting the issue of a birth certificate. The citizen proceeds and provides the MACS with all

the necessary information. The MACS receives the data and, after its storage, it sends a notification to an MoA employee to process the request. When the request has been processed, then citizen receives their birth certificate.

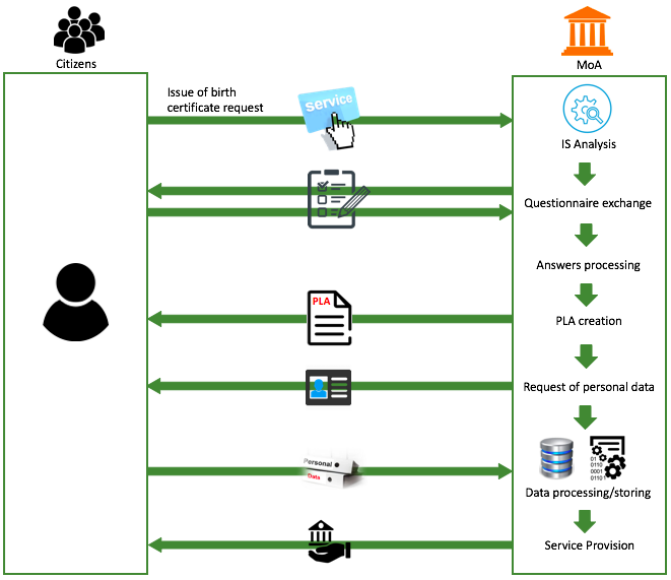

Fig. 2. Process flow of the PLA

The creation of the PLA requires that all fields described in the previous section are filled in with relevant information. Some of the fields (such as the *identity* and *National Public Authority*) can be pre-defined by the PA. Others, such as *Citizen Privacy Preferences*, are filled in based on the answers the citizen provides to the questionnaire. The rest of the fields are filled in following privacy related analysis that PA performs using appropriate tools and systems.

The PLA, depicted in Fig. 3, gives the citizen the ability to be aware of exactly the data the PA has about them, how this data is processed, with whom this data will be shared, the privacy mechanisms implemented by the PA along with the threats that can endanger citizen's privacy and the corresponding mitigation actions. In addition, the citizen knows the PA employee assigned as the data controller of their data, has an estimation of the value of their data and information about past events that enables them to make more informed decisions about the sharing of their data.

5 Conclusions

PAs should realise the importance of the adoption of a privacy culture that enhances their trustworthiness, by making their systems and procedures trans-

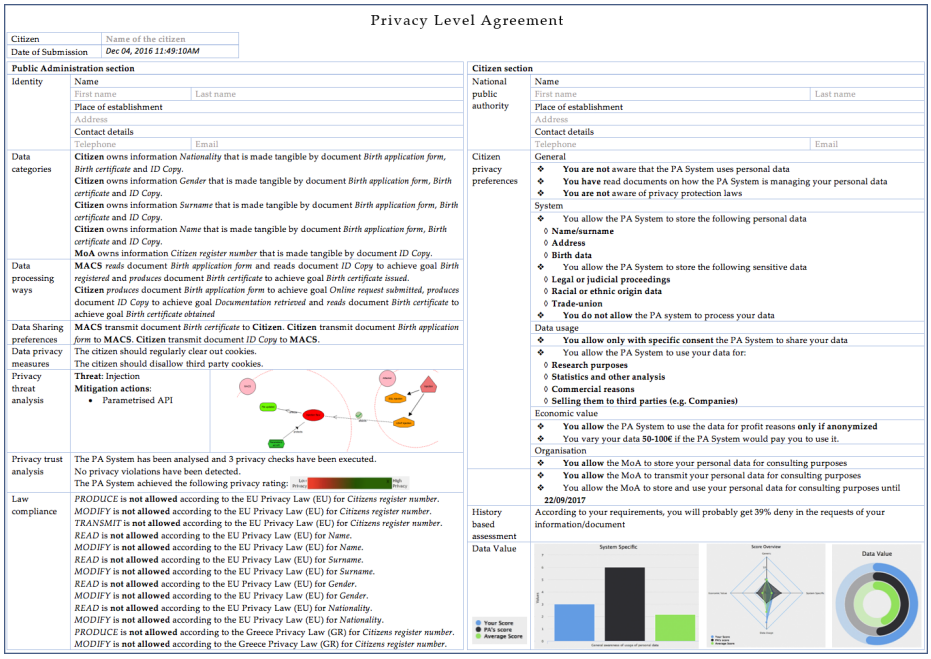

Fig. 3. Instance of a PLA

parent. Towards this goal, the establishment of a PLA can contribute to the achievement of the desired degree of PAs transparency, increasing the awareness of citizens concerning the preservation of their personal data and allowing them to set their preferences concerning the handling of their data.

The idea of PLA can also be applied in other contexts where online services are provided, especially in situations where the provision of individuals' personal data is necessary for the service to be carried out. These contexts can include relationships between healthcare institutions and patients, business to business, and customers to business.

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. Bouman, J., Trienekens, J., Van der Zwan, M.: Specification of service level agreements, clarifying concepts on the basis of practical research. In: Software Technology and Engineering Practice, 1999. STEP'99. Proceedings. pp. 169–178. IEEE (1999)

2. Carter, L., Bélanger, F.: The utilization of e-government services: citizen trust, innovation and acceptance factors. Information systems journal 15(1), 5–25 (2005)
3. Commission, E.: Eurobarometer 431 - data protection report. Tech. rep. (2015)
4. CSA: Privacy level agreement outline for the sale of cloud services in the european union. Tech. rep., Cloud Security Alliance, Privacy Level Agreement Working Group (February 2013)
5. DErrico, M., Pearson, S.: Towards a formalised representation for the technical enforcement of privacy level agreements. In: Cloud Engineering (IC2E), 2015 IEEE International Conference on. pp. 422–427. IEEE (2015)
6. Drogkaris, P., Gritzalis, S., Lambrinoudakis, C.: Employing privacy policies and preferences in modern e–government environments. International Journal of Electronic Governance 6(2), 101–116 (2013)
7. Ebrahim, Z., Irani, Z.: E-government adoption: architecture and barriers. Business process management journal 11(5), 589–611 (2005)
8. Horst, M., Kuttschreuter, M., Gutteling, J.M.: Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in the netherlands. Computers in Human Behavior 23(4), 1838–1852 (2007)
9. Keller, A., Ludwig, H.: The wsla framework: Specifying and monitoring service level agreements for web services. Journal of Network and Systems Management 11(1), 57–81 (2003)
10. Marche, S., McNiven, J.D.: E-government and e-governance: the future isn't what it used to be. Canadian Journal of Administrative Sciences/Revue Canadienne des Sciences de l'Administration 20(1), 74–86 (2003)
11. Milloy, M., Fink, D., Morris, R.: Modeling online security and privacy to increase consumer purchasing intent. In: Informing Science & IT Education Joint Conference (InSITE) (2002)
12. Parliament, E.: 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/`
13. Sedek, K.A., Sulaiman, S., Omar, M.A.: A systematic literature review of interoperable architecture for e-government portals. In: Software Engineering (MySEC), 2011 5th Malaysian Conference in. pp. 82–87. IEEE (2011)
14. Srivastava, S.C., Teo, T.: Citizen trust development for e-government adoption: Case of singapore. PACIS 2005 Proceedings p. 59 (2005)
15. Tambouris, E., Archetypon, S., Wimmer, G.M.: Online one-stop government: A single point of access to. Electronic government strategies and implementation p. 115 (2004)
16. (W3C), W.W.W.C.: Platform for privacy preferences (p3p) project (2016), `https://www.w3.org/P3P/`
17. Welch, E.W., Hinnant, C.C., Moon, M.J.: Linking citizen satisfaction with e-government and trust in government. Journal of public administration research and theory 15(3), 371–391 (2005)