A Metamodel for GDPR-based Privacy Level Agreements

Vasiliki Diamantopoulou, Konstantinos Angelopoulos, Michalis Pavlidis, and Haralambos Mouratidis

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

Abstract. The adoption of the General Data Protection Regulation (GDPR) is a major concern for data controllers of the public and private sector, as they are obliged to conform to the new principles and requirements managing personal data. In this paper, we propose that the data controllers adopt the concept of the Privacy Level Agreement. We present a metamodel for PLAs to support privacy management, based on analysis of privacy threats, vulnerabilities and trust relationships in their Information Systems, whilst complying with laws and regulations, and we illustrate the relevance of the metamodel with the GDPR.

Keywords: Privacy Level Agreement, Metamodel, General Data Protection Regulation, Privacy Management, Privacy Engineering

1 Introduction

Over the last decade, governments have given special attention and have focused their efforts towards the compliance of their services with the Open Government standards, as this will ultimately result in a democratisation of decision-making [1], taking advantage of the advancements in Information and Communication Technologies. Open Government promotes the idea that citizens should have access to understandable, accurate, reusable, auditable data and information about government operations and decision making, where transparency [15] and the presence of mechanisms for public scrutiny and oversight are in place, with an emphasis on government accountability. In such context, privacy preservation represents an important public value for Open Government and the increased use of e-services has raised issues about the privacy of the information provided by the citizens and about the sharing of that information [13, 8, 20].

A recent European Commission (EC) initiative for capturing European citizens' opinion concerning their attitude to data protection [2] 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. The same survey reveals that 58% are convinced that they are obliged to provide personal information in order to benefit from online products and services, while 52% are sceptical about the provision of personal information in return for online services. This survey makes

In: C. Cabanillas, S. España, S. Farshidi (eds.):
Proceedings of the ER Forum 2017 and the ER 2017 Demo track,
Valencia, Spain, November 6th-9th, 2017,
published at http://ceur-ws.org

clear that a big share of citizens still remains reluctant of using online services, adding another obstacle to the wide adoption of e-government services. Citizens' unawareness concerning the handling of their personal data is enhanced by the fact that the monitoring of personal information is ubiquitous; while the data storage is so durable as to render one's past undeletable [11]. The General Data Protection Regulation (GDPR) [16] that forces organisations to manage data in a specific way with regards to privacy reinforces all the above.

This work proposes a metamodel that captures the privacy-related entities mentioned in the GDPR and the relationships among them, and allows the designers of e-services to better understand the concepts that must be included in a PLA. The reminder of the paper is set out as follows: Section 2 discusses related work while Section 3 presents the conceptual language of a PLA. Finally, Section 4 concludes the paper by raising issues for further research.

2 Related Work

Work on PLAs has been limited so far. The Privacy Level Agreement Working Group of the Cloud Security Alliance (CSA) has defined a PLA in the context of cloud services [3]. Similarly, the concept of PLA has been presented by [5] as a standardised way for cloud providers to describe their data protection practices. In the same way to the CSA proposal, this work focuses on the cloud environment and 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.

The authors in [6] propose an architecture that promotes the employment of privacy policies and preferences. They introduce the Privacy Controller Agent for storing and comparing service providers' privacy policies and user privacy preferences. However, this work does not provide an agreement between two entities (e.g., PA and citizens) but rather an architecture to define privacy policies.

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 [9]. In contrast to the PLA concept, an SLA does not take into account privacy aspects of the agreement between a service provider and a service consumer. sed on their privacy preferences, relevant threats and trust issues along with an indication of the value of their data. PLA will be a clear way that empowers and supports them in deciding about their data and receive warnings about 'bad decisions' or breaches with respect to their privacy.

3 Metamodel of a Privacy Level Agreement

In this section we propose a metamodel that captures the entities mentioned in the GDPR, related to data protection in e-services offered by PAs. This meta-

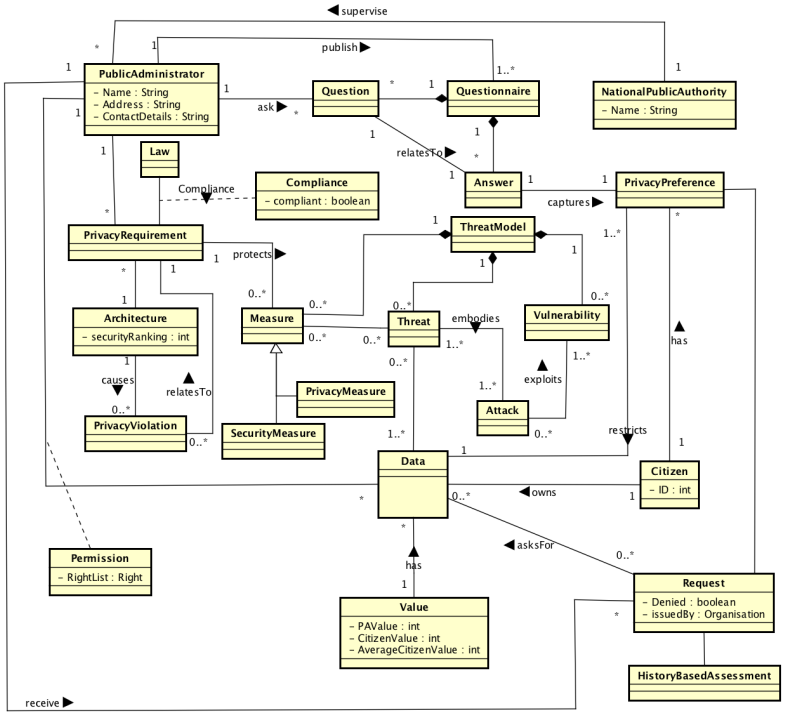

Fig. 1. A metamodel for composing Privacy Level Agreements.

model formalises the relationships of the privacy-related concepts of the GDPR and contributes to the development of digital contracts between PAs and citizens who use their e-services. Words in italics refer to the concepts of the metamodel.

The first concept is the *Public Administrator* (PA) who offers an e-service used by citizens and requires various data from them. A PA is identified by its name, place of establishment and contact details of the PA's data controller administrator. Paragraph 39th of the GDPR states that the identity of the data controller (i.e. PA) to the data subjects (i.e. citizens) should be indicated, to provide transparency. Also, according to the 1st paragraph of the 30th Article of the GDPR, the data controller shall maintain a record providing contact details of the controller administrator. In the context of our work, 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]. Contact details need to include an email address in order the PA to be accessible to citizens [18].

For the elicitation of citizens' privacy preferences, a PA publishes *questionnaires* where each *question* refers to specific data and how it could be managed, e.g., a PA might ask citizens for how long they prefer their data to be stored at the PA's database. Each *answer* captures a privacy preference of a citizen which

restricts the data they share with a PA. The government applications that engage citizens and allow interactivity with them have positive payoffs for trust in government [21]. Additionally, the 70th paragraph of the GDPR highlights the processing of personal data for marketing reasons and describes explicitly citizens' right to consent or not. According to the 156th paragraph of the GDPR, a citizen should be fully aware of the purposes of their data sharing, and this should be subject to appropriate safeguards for the rights and freedoms of the them.

Citizen's *data* is also *requested* by external organisations. Therefore, some of the citizen's privacy preferences are related to the *permission* of sharing their data with these organisations or not. Based on this, a request can be either allowed or denied. According to the 4th paragraph of the 30th Article of the GDPR, the data controller shall maintain a record providing the categories of recipients to whom the personal data have been or will be disclosed, i.e. recipients in third countries or international organisations. The 82nd paragraph of the GDPR mentions that the PA should maintain records of processing activities concerning citizens' personal data. Moreover, in [4] it is argued that history events can influence trust of an individual. This information can support the citizens in taking better decisions concerning the sharing of their data with the PA. Hence, a *history-based assessment* shall be associated with each piece of data that is exposed to requests from external organisations. This type of 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 amount of requests for the citizens' data that have been allowed or denied, based on their requirements available and the aggregated statistics about other citizens, collected up to that moment.

Another important aspect of privacy that GDPR targets is citizens' awareness about the *value* of their data. To improve awareness, data shall be associated with three values. The first value captures citizens' valuation, the second captures the valuation by the PA, and the third captures the average valuation of all the citizens. These values represent the relative importance of the provided information with respect to how sensitive this information is, given that citizens have not yet acquired critical thinking on which data they should share [19]. This information will increase citizens' awareness about how their data is used, as well as their criteria to assess and control the level of risk for their privacy. Consequently, it is expected that citizens will gain useful insights on the value of their digital personal data. In addition, by providing information to the PA about the value of the collected data that has been assigned by the citizens, it will allow better decision making for the PA.

PAs have certain requirements about how to handle citizens' privacy in the context of their services. Such requirements constrain the operations that PAs perform on the citizen's data (e.g., transmit, modify, read, etc.). For example, when transmitting digitally a document from one organisation to another, the communication channel should satisfy confidentiality constraints, e.g., by using encryption. Additionally, the PA operations should be compliant with existing

laws and communicated to the citizens. According to the 23rd and the 60th paragraphs of the GDPR it is necessary to ensure citizens' consent for the processing of their personal data. Acquiring complete information about processing and storing of their data to the PAs' information systems, citizens are fully informed, e.g., on the location of their stored data, on the processing ways, etc. Also, this field answers to the demand of the 42nd paragraph of the GDPR for the proof of citizens' consent. Furthermore, the *compliance* of the operations performed by PAs should be communicated to citizens. In particular, the 81st paragraph of the GDPR refers the adherence to an approved code of conduct or an approved certification. Law compliance is one of the factors that makes an environment feel safe and trustworthy for the citizen [12].

A recent survey conducted by the EC [2] showed that only 37% of the European citizens are aware of a *National Public Authority* responsible for protecting their personal data rights. Adding such information to the PLA will raise citizens awareness regarding the protection of their data rights by the specific Authority.

From a technical point of view, the *architecture* of the PA systems must be compliant with the *privacy requirements* of the PA. This should be demonstrated to the citizens before deciding to consent sharing their data with PAs, in order to enhance their trust [7, 14]. The 83rd paragraph of the GDPR highlights the importance of the maintenance of the data security, attributing this responsibility to the PA for the evaluation of the risks inherent in the processing and for the implementation of measures to mitigate the identified risks, ensuring an appropriate level of security.

The 78th and the 84th paragraphs of the GDPR describe the concern of PAs to ensure the protection of citizens' personal data by adopting appropriate technical and organisational *measures*, presenting specific actions to be implemented. The adoption of internal policies and the implementation of measures will meet the principles of data protection-by-design and by-default. To avoid *privacy violations* from the PA's system architecture, a security analysis should precede the system's design. Therefore, the metamodel includes the *threat model* concept that is composed of the PA system's *vulnerabilities*, *threats* and *attacks* that potentially could exploit them, as well as the countermeasures that are implemented to defend the system.

The 83rd paragraph of the GDPR highlights the importance of the maintenance of the data security and privacy, attributing this responsibility to the PA for the risks evaluation inherent in the processing and for the implementation of *security* and *privacy measures* to mitigate the identified risks, ensuring an appropriate security level.

Finally, citizens need assurances that the PA introduces appropriate mechanisms and processes to support the privacy needs, and informs them when these needs are not followed, due to either PA policies or legislation. Such information improves the transparency of PA's operations in terms of data management, and it therefore contributes to citizens' trust improvement. The existence of secure systems and the communication of the security related information to the citi-

zens can contribute to the development of citizen trust towards the PA and its systems [17].

4 Conclusions

This work proposes a metamodel to describe the privacy-related concepts mentioned in the GDPR, which allows designers of e-government services to compose PLAs. The adoption of PLAs will enhance citizens' trust, since there is a formal agreement that guarantees that citizens privacy preferences are respected. Furthermore, our proposal allows the creation of digital contracts that can be used by the PAs e-services to enclose, monitor and enforce citizens privacy preferences. Given that our proposal is based on the current version of the GDPR, the metamodel allows every time a new article is introduced or changed, to identify the overall changes in the domain and the impact that might have in the objectives of the PLA.

Future directions include the identification of appropriate methods and tools that will enable PAs to capture the necessary information during the design time of the PA system and also to support run-time privacy protection. The above can later be validated through a real case study. Moreover, we plan to provide a tool that will receive as input a more detailed version of our metamodel and automatically produce the schema of a PLA. This way we target to standardise the creation of PLAs and therefore, improve interoperability when PLAs need to be merged due to an expansion of an e-service or the union of two PAs their format will be identical.

References

1. Carter, L., Bélanger, F.: The utilization of e-government services: citizen trust, innovation and acceptance factors. Information systems journal 15(1), 5–25 (2005)
2. Commission, E.: Eurobarometer 431 - data protection report. Tech. rep. (2015)
3. 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)
4. Daskapan, S., Vree, W.G., Eldin, A.A.: Trust metrics for survivable security systems. In: Systems, Man and Cybernetics, 2003. IEEE International Conference on. vol. 4, pp. 3128–3135. IEEE (2003)
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. 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)

8. Irani, Z., Kamal, M., Carter, L., McBride, A.: Information privacy concerns and e-government: a research agenda. Transforming Government: People, Process and Policy 4(1), 10–13 (2010)
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. Mayer-Schönberger, V.: Delete: The virtue of forgetting in the digital age. Princeton University Press (2011)
12. McKnight, D.H., Choudhury, V., Kacmar, C.: Developing and validating trust measures for e-commerce: An integrative typology. Information systems research 13(3), 334–359 (2002)
13. McRobb, S., Stahl, B.C.: Privacy as a shared feature of the e-phenomenon: a comparison of privacy policies in e-government, e-commerce and e-teaching. International journal of information technology and management 6(2-4), 232–249 (2007)
14. 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)
15. Obama, B.: Transparency and open government. Memorandum for the heads of executive departments and agencies (2009)
16. Parliament, E.: 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) (2016), `http://eur-lex.europa.eu/legal-content/EN/TXT/`
17. Srivastava, S.C., Teo, T.: Citizen trust development for e-government adoption: Case of singapore. PACIS 2005 Proceedings p. 59 (2005)
18. Torres, L., Pina, V., Acerete, B.: E-government developments on delivering public services among eu cities. Government Information Quarterly 22(2), 217–238 (2005)
19. Tuunainen, V.K., Pitkänen, O., Hovi, M.: Users' awareness of privacy on online social networking sites-case facebook. Bled 2009 Proceedings p. 42 (2009)
20. Vrakas, N., Kalloniatis, C., Tsohou, A., Lambrinoudakis, C.: Privacy requirements engineering for trustworthy e-government services. In: International Conference on Trust and Trustworthy Computing. pp. 298–307. Springer (2010)
21. 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)