International Journal of Electronic Government Research
Volume 18 • Issue 1

A Privacy-by-Design Implementation Methodology for E-Government

Anton A. Gerunov, Sofia University "St. Kliment Ohridski", Bulgaria*

ABSTRACT

The issues of privacy and data protection are gaining in prominence, especially against the backdrop of changing citizen preferences and the enforcement of strict legislations such as the EU's General Data Protection Regulation. Pursuant both article 25 of the regulation and following good practice, public sector institutions need to apply the principle of privacy by design (PbD) to their information systems. However, there is limited consensus on how this application is to be carried out. This article aims to fill this gap by constructing an implementation methodology with a particular focus on the e-government domain. This is done by using a design science approach leveraging practical experience and extant literature to design the methodology in accordance to user needs, existing legal requirements, and best practices. The proposed new methodology is applied to a real-life project from Bulgaria's e-government roadmap and evaluated by project stakeholders and experts.

KEYWORDS

Data Protection, E-Government, GDPR, Methodology, Privacy by Design

INTRODUCTION

Issues of information security and privacy has gained significant interest and salience among both academic and practitioners. Protecting personal data is not only increasingly seen as a potential competitive advantage but also mandated by ever stricter regulations such as European Union's General Data Protection Regulation and the numerous US privacy regulations. One of the important problems to implementing privacy controls has been to operationalize the requirements and apply them in the most cost-effective way. Cavoukian (2010) has proposed that in order to do that privacy needs to be introduced at the very early stages of information systems development, and this set of principles is known as the Privacy by Design (PbD) approach to personal data protection. The particularities of applying the PbD principles to real-life projects, however, remains unclear, and numerous approaches persist (Semantha et al., 2020). The challenge is particularly pertinent in the public sector which calls for a specific methodology that is both suitable for e-government applications and flexible enough to accommodate the requirements of a large scope of potential government and municipal users.

The goal of this work is thus to present a suitable methodology that can guide the implementation of the Privacy by Design principles in the e-government domain. This methodology builds upon existing Software Development Life Cycle (SDLC) methodologies and adds to them phases that are specific for the e-government domain such as a more stringent legal analysis, as well as public consultation with relevant stakeholders. To illustrate its application a particular real-life project from the Bulgarian e-governance roadmap is selected and modeled using standard Unified Modeling Language (UML) notation with privacy enhancements. This is then presented to six experts working on this project and evaluated via in-depth semi-structured interviews. The results shed more light

DOI: 10.4018/IJEGR.288067 *Corresponding Author

on how the principles of PbD are understood and what concrete practices can be used for their application. The article proceeds as follows. The second section provides a short literature review of PbD design principles and implementation methodologies. The third section is an overview of the methodological approach that largely follows the Design Science (Hevner et al., 2004) paradigm, and the fourth section presents the outlines of the newly proposed methodology. Section five shows how it can be used to a real-life e-government project, while section six discusses the results and concludes.

BACKGROUND

Provide broad definitions and discussions of the topic and incorporate views of others (literature review) into the discussion to support, refute, or demonstrate your position on the topic.[1] The need for rigorous information security and privacy functionalities in the e-government domain is hardly a new development (Ebrahim & Irani, 2005). However, the increasing scope and complexity of government functions, together with rising public concern and more aggressive regulations such as the European Union's GDPR, have increased the salience and the need for ever better privacy measures. While it is widely agreed that implementing security and privacy controls at the design stage of a given information system significantly minimizes work, increases security, and decreases costs (Williams, 2009; Schaar, 2010, Hustinx, 2010), it remains unclear exactly how to do so in a realistic setting (Kroener & Wright, 2014, Jacobs & Popma, 2019, Bednar et al., 2019). Cavoukian (2012a) has proposed a number of principles that Hoepman (2014) operationalizes in a number of privacy-preserving strategies and tactics. Some authors use those to propose a PbD methodology (e.g. Dennedy et al, 2014; Cronk, 2018) but those efforts are largely focused on the private sector.

OVERALL FRAMEWORK

A Privacy by Design (PbD) implementation methodology for e-government can only be effective by simultaneously addressing the multitude of dimensions that a software development project entails – both technological and social-organizational ones. The success of a given IT artefact depends not only on appropriate technology but also on its embeddedness in the organizational structure and its ability to integrate with and support norms and behaviors. the Socio-Technical Model (STM) may be leveraged as a useful framework that reflects this multitude of dependencies (see e.g. Kowalski, 1994; Østby et al., 2019). The Technological dimension of the STM focuses on the Machines (infrastructure) and the Methods (operations) performed upon them. The social dimensions include both the formal structure of the organization (formal and process-wise), as well as the culture (ethical and legal dimensions) that support behaviors, norms and expectations. The successful implementation of a Privacy by Design initiative necessarily hinges upon all aspects – it must operate on the IT infrastructure but also include rules, and design patterns of higher order. Equally important, the process must be formalized within the official structures of the organization but also understood and supported by the professionals that are directly or indirectly involved in it. The importance of individual-level and socio-organizational considerations as success factors for digital transformation efforts is now well established (Grublješič et al., 2019). While implementations have largely focused on deriving concrete software requirements (Morales-Trujillo et al., 2019), e-government applications require a much more involved multi-stakeholder approach and thus all elements of the STM must be properly addressed to ensure success. We begin by reviewing the PbD foundational principles and then show how existing methodologies need to be expanded to more fully account for the specific needs of electronic government information systems.