

Towards Privacy Preservation and Data Protection in Information System Design

An introduction to the special issue

Agnes Koschmider^{*,a}, Judith Michael^b, Nathalie Baracaldo^c

^a Kiel University, Group Process Analytics, Germany

^b RWTH Aachen University, Software Engineering, Germany

^c IBM Almaden Research Center, San Jose, CA, USA

Abstract. *This paper serves as an editorial to the corresponding special issue setting out solutions and future directions of privacy preservation and data protection in information system design.*

Communicated by Agnes Koschmider.

1 Introduction

This special issue seeks research articles, industry or experience reports related to all aspects of privacy and data protection in the design of information systems. Data breaches and data misuse continuously increase the uncertainty in the use of devices and systems that process personal data. Apart from this, declarations of consent are given by users without a clear understanding of it or even without reading the declarations. Sensitive information, such as personal data must be given special attention when designing information systems. Personal data protection is of paramount importance to ensure compliance with the General Data Protection Regulation (GDPR), which obliges organizations to consider privacy throughout the complete development process. This requires an interplay between technical solutions related to privacy engineering techniques and user-friendly interfaces allowing to protect data and to configure privacy preferences by users. This is also critical to build information systems that users can trust.

The purpose of this special issue was to discuss approaches related to privacy-by-design, privacy

engineering, privacy enhancing technologies, privacy architectures, the integration of privacy into software engineering lifecycle phases, user experience with privacy mechanisms, data protection in analytics and mining or investigating privacy concerns within agile (or) model-based system engineering methods and to extend the body of related papers (Baracaldo et al. 2018; Mannhardt et al. 2019; Michael et al. 2019a,b).

Two papers have been accepted for the special issue: “*Personal data management inside and out: Integrating data protection requirements in the data life cycle*” authored by C. Labadie and Ch. Legner and “*DPMF: A Modeling Framework for Data Protection by Design*” authored by L. Sion, P. Dewitte, D. Van Landuyt, K. Wuyts, P. Valcke and W. Joosen.

The first paper systematically analyzes the GDPR and the CCPA and identifies their implications on the data life cycle. It aims to answer the following two research questions (1) What is the impact of data protection regulations on the personal data life cycle? (2) How could data life cycle models be amended in order to address regulatory requirements for data protection? The second paper presents a data protection modeling framework that allows for a comprehensive and

* Corresponding author.

E-mail. ak@informatik.uni.kiel.de

accurate description of the data processing operations in terms of the key concepts used in the GDPR.

In addition to these two papers, this special issue reports on a panel discussion on “Trust and Privacy in Process Analytics” that took virtual place at the 1st Workshop on Trust and Privacy in Process Analytics (TPPA) co-located with the 2. International Conference on Process Mining.

2 Acknowledge

We would like to thank the reviewers for their comments and effort towards improving the manuscripts.

References

Baracaldo N., Chen B., Ludwig H., Safavi A., Zhang R. (2018) Detecting Poisoning Attacks on Machine Learning in IoT Environments. In: 2018 IEEE International Congress on Internet of Things (ICIOT), pp. 57–64

Mannhardt F., Koschmider A., Baracaldo N., Weidlich M., Michael J. (2019) Privacy-Preserving Process Mining: Differential Privacy for Event Logs. In: Business & Information Systems Engineering (BISE) 61(5), pp. 595–614

Michael J., Koschmider A., Mannhardt F., Baracaldo N., Rumpe B. (2019a) User-Centered and Privacy-Driven Process Mining System Design for IoT. In: Information Systems Engineering in Responsible Information Systems. Lecture Notes in Business Information Processing. Vol. 350. Springer, pp. 194–206

Michael J., Netz L., Rumpe B., Varga S. (Sept. 2019b) Towards Privacy-Preserving IoT Systems Using Model Driven Engineering. In: Model-Driven Engineering for the Internet of Things & Interplay of Model-Driven and Component-Based Software Engineering (MDE4IoT & ModComp 2019). CEUR-WS.org, pp. 15–22