Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 10, Issue 1, 2022

Implementation of privacy by design model to an eHealth information system

Matjaž Drev, National institute of public health, Slovenia, matjaz.drev@nijz.si

Dalibor Stanimirović, Faculty of Public Administration, University of Ljubljana, Slovenia, dalibor.stanimirovic@fu.uni-lj.si

Boštjan Delak, Faculty of Information Studies, Slovenia, bostjan.delak@fis.unm.si

Abstract

This paper reports ongoing research on the process and results of implementing a conceptual model of privacy by design. The model is based on building blocks derived from a comparative analysis of approaches to privacy by design by different authors. We then implemented the model to the data processing operations of Slovenia's central health information system (eHealth). The main goal of our research was to ensure personal data processing compliance with the General Data Protection Regulation (GDPR) and privacy by design criteria set by the model. Findings were used to answer the research questions: whether the proposed conceptual model is general enough to be used in most personal data processing operations, regardless of context; does the successful implementation of conceptual model requirements in personal data processing operations lead to compliance with the GDPR and with the additional requirements of privacy by design, and is the efficiency of complying with personal data processing higher when using the conceptual model compared to other approaches. Current results show that the model is robust enough to be used in a complex system of personal data processing. It also enables a relatively quick assessment of the gap between the actual and target situation, while suggesting which measures should be taken to comply. However, the model still must be tested in several organizations and other contexts of personal data processing, as only a comparative meta-analysis can provide reliable answers to the questions posed.

Keywords: Privacy by design, conceptual model, personal data, information system, eHealth.

Introduction

In the modern information society, increasing emphasis is placed on the field of personal data protection as it expresses the concern for the right to privacy of individuals and represents an effort to comply with legal requirements. Compliance became particularly important in the European Union (EU) after the introduction of the General Data Protection Regulation (GDPR). The United States (U.S.) currently does not have similar legislation on the federal level; however, California Consumer Privacy Act (CCPA) and other similar national Acts show that information privacy is also a concern in non-European countries. Drev and Delak (2021) investigated whether systematic and structured approaches of ensuring the compliance of personal data processing operations exist already. They also sought to determine whether different approaches could be combined into a single conceptual model that would allow relatively simple and transparent compliance with both

the GDPR and the upgraded privacy by design criteria. The purpose of this paper is to present the process of implementing the conceptual model of privacy by design proposed by Drev and Delak, (2021). The first section briefly describes the conceptual model. Section two describes the organizational environment where the model was tested. In section three, the analysis and the results of model implementation on personal data processing operations are presented. The final part consists of the discussion and conclusions.

Conceptual Model of Privacy by Design

Literature Review

The concept of *data protection by design and by default* can be understood as the idea that systems should be designed and constructed in ways that avoid or minimize the amount of personal data processed (Schaar, 2010). Rubinstein (2011) pointed out that building in privacy from the outset when designing information and communications technologies achieves better results than bolting it on at the end. The conceptual model of privacy by design (Drev & Delak, 2021) is based on a comparative analysis of several approaches to understanding privacy. The starting point was Ann Cavoukian's (2009) key principles of privacy by design, which represents the first attempt to conceptualize a notion of privacy by design is. Cavoukian (2009) set out the following principles: proactivity instead of reactivity; privacy as the default choice; privacy, which is an integral part of the design of the solution; full functionality—a game with a positive-sum; data protection throughout the data processing cycle; transparency; respect for the individual. However, Gurses, et al. (2011) criticized the over-generality of these fundamental principles of privacy by design. In their view, the categories set by Cavoukian (2009) are too vaguely defined to be suitable for implementation in personal data processing operations. Thereafter a meta-analysis of several studies done by Huth and Matthes (2019) was reviewed and used. It included studies done by Bellotti and Sellen (1993), Hong et al. (2004), Jensen et al. (2005), Kalloniatis et al. (2008), Spiekermann and Cranor (2009), Deng et al. (2011), Hoepman (2014), Notario et al. (2015). Aditionally, an analysis of the GDPR (2018) was conducted, as the regulation serves as a key reference point for ensuring compliance with personal data protection in the EU.

Conceptual Model

The purpose of the analysis and comparison of different approaches to understanding privacy by design was to determine whether there are elements of personal data protection that are common to all compared approaches. Common elements were identified and used as building blocks of the conceptual model of privacy by design. Elements of the *GDPR model* approach were used as a starting point for developing the conceptual model, because they contain all substantive elements of other approaches and terminology consistent with the GDPR, which is key legislative document in the field of personal data protection, enforced by inspection supervision of each EU member state. To this starting set of elements, additional ones were added, such as the *processing contracts* of personal data between data controllers and processors, and the *Data Protection Impact Assessment (DPIA)* which is mandatory in some cases of data processing. The elements of personal data protection were grouped into one of three sets: “legal elements”, “security elements”, and “privacy by design and by default elements” (Drev and Delak, 2021). The sets are consistent with the structure of GDPR where legal elements, particularly the legal basis for data processing,

occupy a central position, followed by data security, and finally by privacy by design and by default provisions. Such structure was also in line with the extensive audit experiences of the authors.

eHealth Environment

The term *eHealth* is an umbrella name for the components of the central health information system in the Republic of Slovenia (further: Slovenia), developed and maintained by the National Institute of Public Health (NIJZ). The eHealth solutions are intended for an extremely wide range of users, which includes all healthcare providers and all citizens in Slovenia, and are based on the extensive processing of sensitive personal data in a combination of centralized and decentralized modes. The key components of eHealth are, the Central Patient Data Registry (CRPP)—the largest healthcare database in the country, the secure zNET network—an extensive Virtual Private Network (VPN) that connects healthcare providers with CRPP, and various application modules—for example the zVEM web portal which provides all citizens free access to their health data. Based on the information obtained from the eHealth website (https://www.ezdrav.si), internal documentation available on the NIJZ intranet, and interviews with owners of data processing operations, the authors created a diagram of eHealth building blocks and the data flow between them.

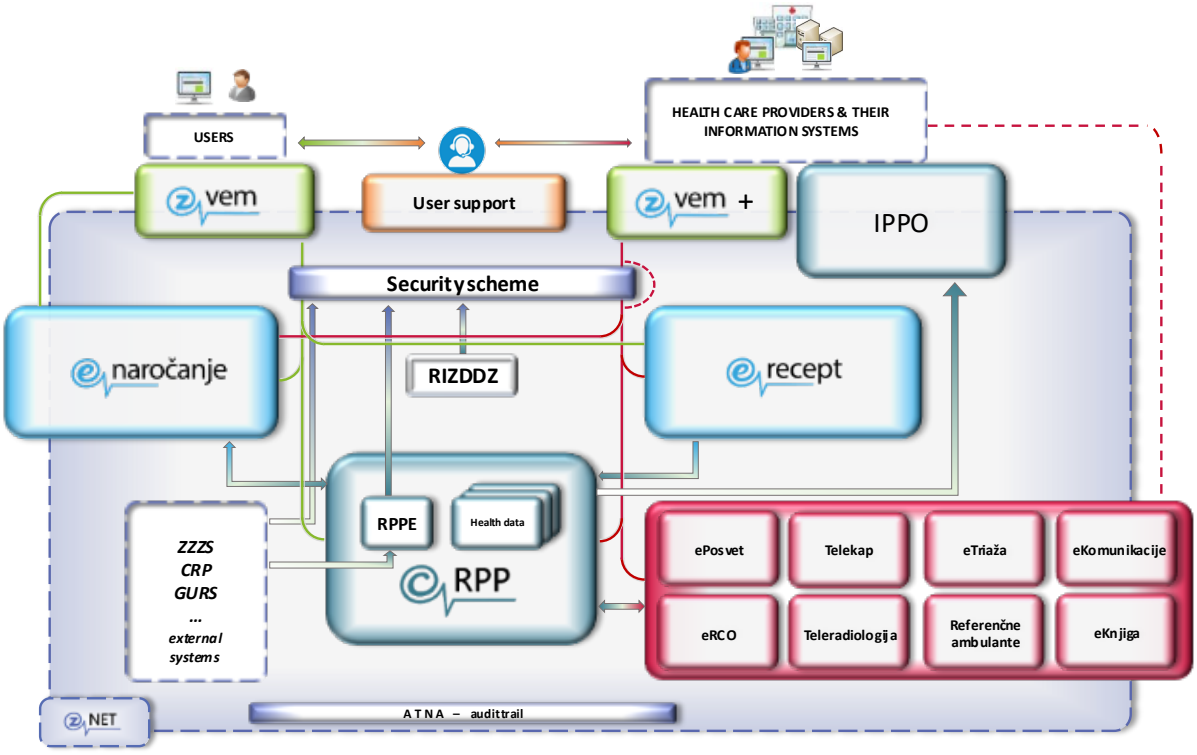

Figure 1. Diagram of Personal Data Processing Operations Within eHealth

As can be seen from Figure 1, eHealth currently consists of the following building blocks: CRPP, eNaročanje, eRecept, zVEM portal, zVEM+ portal, zNET, Varnostna shema, PNP, eTriaža, Teleradioloija, Telekap, eKomunikacije, Referenčne ambulante, IPPO, eRCO, eKnjiga, ePosvet,

RIZZDD. There were several reasons to test the conceptual model on eHealth. It is a complex information system with a central role in the Slovenian healthcare sector. At the same time, it is part of the national critical infrastructure, and its central building block is the largest health database in the country (CRPP) connecting all health care providers and is to some extent accessible by citizens via a web portal and a mobile application. Within the eHealth environment, several modules based on the processing of sensitive personal data that are accessed by healthcare providers over the secure zNET network (the largest virtual private network in the healthcare sector in Slovenia), are developed and maintained. System complexity presents a substantial challenge to testing the model, however, this improves the feasibility of implementation in less complex systems. Since two of the authors are employed by NIJZ, the organization which manages eHealth, detailed insight into the operation of the system was possible. Also, this enabled options to influence management decisions regarding the introduction of corrective measures to achieve a higher level of compliance with the GDPR and privacy by design criteria.

Implementation Procedure

Implementing the model was done in five steps. In Step 1, one author who acted as an auditor got the information, namely a review of the website (www.ezdrav.si) material, internal documents describing the functioning of each specific personal data processing operation, interviews with the management of the Information Technology (IT) center, the Data Protection Officer (DPO), and the administrators of all analyzed processes. Representatives of data processors were also interviewed for information. The questionnaire developed by the authors guided the whole process of information gathering. In Step 2, the authors analyzed the information thus obtained in terms of the presence of legal elements derived from the model and scored these elements according to the proposed descriptive matrix, with scores ranging from 1 to 4 for each. In Step 3, the authors repeated the procedure for the security elements. There were several complications here, as the GDPR is not clear on assessing when the level of data security is appropriate. Therefore, a starting point in the assessment was the international standard, ISO/IEC 27001:2013, specifying individual elements of information security. At that point, the authors faced a major dilemma regarding how specific the descriptive matrix for security elements should be. Complex organizations and processes often require more extensive security measures. However, going the route of introducing numerous criteria in a way ISO/IEC standard does, would reduce the generality of the model and its usefulness for a smaller and simpler organizations. Therefore, authors took a simpler approach to security with a smaller number of criteria. By taking this approach, the privacy by design model should be easier and more flexible to use, although at the cost of precision when determining the level of information security. During this phase some security procedures, which are formally written as policies, had to be checked at the operational level, to ensure that security measures are at least to some extent enforced into practice However, the authors have not yet reached a consensus on the optimal number and extent of such security probing. In Step 4, it was determined whether elements of privacy by design and by default were present. The GDPR only briefly outlines these, so the more precise international standard, namely ISO/IEC 27701:2019, governing the protection of personal data, was used as a measuring tool. Defining and scoring these elements has proved to be a major challenge because of their vagueness. The same author completed Steps 1 to 4, as this approach seemed to yield the most consistent results. We completed Step 5

comprising an analysis of the gap between the actual state and the target state, recommendations for closing the gap, and the final report with all the findings. Implementing all the steps took 32 working days (from January 2021 to April 2021), as shown in Table 1.

Table 1. The sequence of steps when implementing privacy by design model

Sequence of Steps	Step description	Used time
1 Information gathering	Information was gathered from legal documents, company website, intranet, internal documents, Data Privacy Impact Assessment (DPIA), contracts with processors, interviews with the head of the informatics center, Data Protection Officer (DPO), IT administrators, security consultant, process owners, and data processor contract managers. Personal data processing operations and registers were then determined.	12 days
2 Analysis of legal elements	Information was analyzed for the presence of legal elements. All found elements were appropriately listed and marked. Analysis was performed in the following sequence: Determining the purpose of data processing. Finding an appropriate legal basis for data processing. Determining how the transparency of data processing is ensured. Determining mechanisms for exercising the rights of individuals according to GDPR. Determining how contractual (external) processing is arranged.	4 days
3 Analysis of security elements	Information was analyzed for the presence of security elements. All found elements were appropriately listed and marked. Each data process was checked from the viewpoint of ensuring proper confidentiality, integrity, and availability of personal data. Audit measures were also checked.	6 days
4 Analysis of privacy by design and by default elements	Information was analyzed for the presence of privacy by design and by default elements. All found elements were appropriately listed and marked. Analysis was performed in the following sequence: Determining how data encryption is ensured both when transferring and storing data. Determining if and how data minimization is ensured. Determining if and how data pseudonymization is ensured. Analysis of (existing) DPIA.	6 days
5 Final Report with gap analysis and recommendations	Doing gap analysis (difference between the actual state of data processing and benchmarks). Preparing recommendations for assuring a higher level of compliance. Preparing and presenting a final report.	4 days

Table 2 shows all analyzed personal data processing operations, which elements of personal data protection are present, and what values they hold. These are important for assessing the degree of compliance with a distinction between basic (*GDPR*) compliance and upgraded (*privacy by design*) compliance. Basic compliance is achieved if most legal and security elements individually score at least 3-points and most of the privacy by design and by default elements at least 2-points.

However, if most elements score 4-points, except for the privacy by design and by default elements, where three points would be sufficient, upgraded compliance is reached. From the point of view of compliance with the GDPR, at least the basic level is required or the processing processes do not comply with the legislation.

Table 2. Presence of Elements and Consistency of Data Processing Processes

Processing operation / presence of privacy by design model elements Legend: 1 – element not present 2 – element is present, mayor inadequacy 3 – element is present, minor inadequacy 4 – element is fully present / - no personal data processing or part of another filling system	**Legal elements**				**Security elements**			**Data protection by design and by default**			**Compliance**	
	Legality of processing	Informing individuals	Rights of individuals	Processing agreement	Confidentiality	Integrity	Accessibility	Encryption	Pseudonymity	Data minimization	Basic (GDPR)	Upgraded (PbD)
CRPP	4	4	4	4	4	4	4	3	2	3	YES	NO
eNaročanje	4	4	4	3	4	4	4	3	2	3	YES	NO
eRecept	4	4	4	4	4	4	4	3	2	3	YES	NO
portal zVEM	/	4	4	3	3	4	4	3	2	3	/	/
portal zVEM+	/	3	3	3	3	3	4	3	2	3	/	/
zNET	4	4	4	3	4	4	4	3	2	2	YES	NO
Varnostna shema	4	3	4	3	4	3	4	3	2	2	YES	NO
PNP	3	3	4	4	4	4	4	3	2	2	YES	NO
eTriaža	4	4	4	4	4	3	4	3	2	3	YES	NO
Teleradiologija	4	4	4	3	4	3	4	3	2	3	YES	NO
Telekap	4	4	4	3	4	3	4	3	2	3	YES	NO
eKomunikacije	4	3	3	4	4	4	4	3	2	3	YES	NO
Referenčne ambulante	4	4	4	3	4	3	4	3	2	3	YES	NO
IPPO	/	3	4	3	4	3	3	3	2	3	/	/
eRCO	4	4	4	3				3	2	3	YES	NO
eKnjiga	/	4	3	/	3	3	3	3	2	2	/	/
ePosvet	/	4	4	/	3	3	3	3	2	2	/	/
RIZZDD	3	3	4	3	4	3	3	3	2	3	YES	NO

Findings

Based on the information collected and analyzed, it was found that 13 personal data processing operations achieved the basic level of compliance required by the GDPR. However, five (5) operations were not directly linked to personal data filling systems, but acted as proxies for other operations, therefore they did not receive the final assessment. None of the operations fulfilled the stricter criteria of the upgraded "*privacy by design*" benchmark, so perhaps the upgraded compliance benchmark is set too high. In some instances of data processing operations, various limiting factors prevented the thorough implementation of privacy by design and by default

elements. As for findings, most personal data processing operations within eHealth scored high on legal and security elements. This is to be expected since the legal basis for data processing in eHealth is defined by national legislation and organizations implement security measures at the start of project development. While EU states use national legislation to enforce stricter rules regarding data privacy in the healthcare sector, the U.S. follows a sectoral approach to achieve the same goal, for example, with the enforcement of the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act. However, despite the relatively high level of data privacy and security, recommendations were made about ways to inform individuals about data processing. Also, to some extent, data processing contracts with outside contractors could be improved. Improvements should be made in security measures, by providing a more extensive audit of the data processed. Encryption measures are implemented well, since all personal data are processed within the zNET encrypted network, however, most data are not encrypted when stored. Improvements could be made on data anonymization on and minimization, as it was found that sometimes more data is collected than is necessary.

Discussion

The article presents an implementation of a conceptual model of privacy by design on a selected case study. The research was mostly application-oriented, to ensure compliance of personal data processing within the eHealth information system with the basic requirements of the GDPR and additional requirements of privacy by design and by default. The paper also tries to answer three key research questions regarding the general applicability of the model, its ability to identify the gap between actual and desired states, and whether it is more effective than other approaches. Based on one case study, it is difficult to assess whether the conceptual model is general enough to be used in all cases of personal data processing. However, the efficiency and relative simplicity of the model tested on a complex information system comprising numerous personal data processing operations, at least indicates that it is applicable in a wide variety of circumstances, such as implementation procedures, data processing compliance assessment and procedure of making recommendations are broad. Therefore, the extent of data processing, context, and associated complexity does not play a decisive role. Several case studies will need to be carried out in the future and the results summarized in a comparative meta-analysis, as only that will offer an answer whether the conceptual model is general enough to be used in all circumstances of personal data processing. This study showed that implementing the model enables determining the actual state of personal data processing operation within the context of privacy protection, and it also allows assessing the gap between the actual state, GDPR requirements (basic compliance), and additional privacy by design and by default requirements (upgraded compliance). Implementation of the model also made it possible to determine the measures that the organization should take to achieve a higher level of compliance. One should note that the actual assessment of the situation largely depends on the quality and reliability of the information obtained. This is especially true for assessing the level of organizational and technical security of data, which is often well regulated on the level of formal data security policies, but less so on the actual operational level. Also, implementing corrective measures largely depends on the support of management and the constructive participation of data processing operations owners. Otherwise,

the measures remain mere recommendations, which do not help to achieve a higher level of compliance with the conceptual model.

Determining whether compliance of personal data processing operations with the GDPR or with upgraded privacy by design and by default requirements depends on the approach used (for example, unstructured *ad hoc* approach, DPIA implementation approach, or use of other conceptual models) proves a greater challenge. It is possible to determine that there is a difference in the degree of (non) compliance with the GDPR requirements before and after introducing the model, however, that does not mean that other models would not be effective. It could prove useful to test other existing approaches empirically, for example, the Privacy Maturity Model (AICPA/CICA, 2011) and the Privacy Impact Assessment method (CNIL, 2018), while adhering to recommendations set by the privacy guidelines prepared by ENISA (2014) and the European Data Protection Supervisor (2018). Efficiency is difficult to measure, as it requires quantitative indicators. For example, one could use a comparison of identified irregularities within inspection supervisions before and after the introduction of the model as indicators. Similarly, the number of detected incidents in data protection, rapid resolution of individuals' requests regarding their data, or the number of complaints received by the organization doing personal data processing could be used as indicators. Another possibility would be to use the number and consequences of detected cyber security incidents as a proxy. Implementation of the privacy by design model implies compliance with information security standards that should lead to an overall decrease in cybersecurity-related risks (Bhatia et al., 2016). Although it was possible to get most of the relevant data during the research, it is insufficient and perhaps too little time passed since introducing the model and the research to make a proper comparison. However, the results show that introducing the model made it possible to identify inconsistencies, even though the processing of personal data within eHealth is relatively well regulated and that even the DPIA was carried out. This outcome shows the need for a conceptual model as a tool for upgrading the level of personal data protection in the chosen organization relatively quickly and effectively in a way that goes beyond both the spontaneous ad hoc approach and the DPIA-based approach.

Conclusion

The implementation of the conceptual model of privacy by design on the operations of personal data processing within the eHealth information system is important from a practical and theoretical perspective. From a practical perspective, because it shows that using the proposed model, with the appropriate support of the organization's management and process owners, it is possible to analyze the actual situation in the area of personal data protection quickly. It is also possible to determine the gap between the actual and target situation, and the measures needed to comply with either the basic GDPR requirements or the upgraded privacy by design model requirements. From a theoretical point of view, the case study is important because it provides partial answers to the research questions, whether the proposed conceptual model is sufficiently general for different contexts of personal data processing, whether it allows determining the actual situation of personal data processing and related identification of compliance with the target state, and whether it allows more effective data protection against alternative approaches. One should emphasize a few weaknesses of the proposed approach. First, results depend on the quality of information gathered and on the specific knowledge and experience of the auditor. Second, the model could prove too

vague to properly assess the actual situation, especially in the presence of information security elements which can be relatively complex. And third, the descriptive matrix used for scoring the elements could be improved. To address some of those potential weaknesses, the model will have to be tested in several organizations and different contexts of personal data processing, as only a comparative meta-analysis will provide a reliable answer to the dilemmas and questions posed. The current results for now are encouraging.

References

American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants. (2011). *Privacy maturity model*. https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

Bellotti, V., & Sellen, A. (1993). Design for privacy in ubiquitous computing environments. *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW '93*, 77–92. https://doi.org/10.1007/978-94-011-2094-4_6

Bhatia, J., Breaux, T., Friedberg, L., Hibshi, H., & Smullen, D. (2016). Privacy risk in cybersecurity data sharing. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security October 2016*, 57-64. https://doi.org/10.1145/2994539.2994541

California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST). (2018). https://oag.ca.gov/privacy/ccpa

Cavoukian, A. (2009). *Privacy by design. The 7 foundational principles*. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Commission Nationale de l'Informatique et des Libertés. (2018). *Privacy impact assessment (PIA): Methodology*. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

Deng, M., Wuyts, K., Scandariato, R., & Wouter, B. P. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfilment of privacy requirements. *Requirements Engineering, 16*(1), 3–32. https://doi.org/10.1007/s00766-010-0115-7

Drev, M., & Delak, B. (2021). Conceptual model of privacy by design. *Journal of Computer Information Systems*, 62(5), 888-895. https://doi.org/10.1080/08874417.2021.1939197

European Union Agency for Cybersecurity. (2014). *Privacy and data protection by design - from policy to engineering*. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

European Data Protection Supervisor. (2018). *Opinion 5/2018. Preliminary opinion on privacy by design*. https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

Gurses, S., Troncoso, C., & Diaz, C. (2011). *Engineering privacy by design*. https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf

Health Insurance Portability and Accountability Act of 1996 (HIPAA). (1996). https://www.cdc.gov/phlp/publications/topic/hipaa.html

Health Information Technology for Economic and Clinical Health Act (HITECH). (2009). https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

Hoepman, J.-H. (2014). Privacy design strategies. *Proceedings of the IFIP International Information Security Conference, Berlin, Heidelberg: Springer*, 446–459. https://doi.org/10.1007/978-3-642-55415-5

Hong, J. I., Ng, J. D., Lederer, S., & Landay, J. A. (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. *Proceedings of the 2004 Conference on Designing Interactive Systems Processes, Practices, Methods, and Techniques - DIS '04*, 91. https://doi.org/10.1145/1013115.1013129

Huth, D., & Matthes, F. (2019). Appropriate technical and organizational measures: Identifying privacy engineering approaches to meet GDPR requirements. *Proceedings of the 2019 American Conference on Information Systems*. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/5

International Organization for Standardization. (2013). *ISO/IEC 27001:2013*. www.iso.org.

International Organization for Standardization. (2019). *ISO/IEC 27701:2019*. www.iso.org.

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. *Requirements Engineering, 13*(3), 241–255. https://doi.org/10.1007/s00766-008-0067-3

Notario, N., Crespo, A., Martin, Y. S., Del Alamo, J. M., Metayer, D. Le, Antignac, T., Kung, A., Kroener, I., & Wright, D. (2015). PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. *Proceedings of the 2015 IEEE Security and Privacy Workshops, SPW 2015*, 151–158. https://doi.org/10.1109/SPW.2015.22

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). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Rubinstein, I. S. (2011). Regulating privacy by design. *Berkeley Technology Law Journal, 26*(3), 1409-1456. https://doi.org/10.15779/Z38368N

Schaar, P. (2010). Privacy by design. *Identity in the Information Society, 3*, 267–274. https://doi.org/10.1007/s12394-010-0055-x

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering, 35*(1), 67–82. https://doi.org/10.1109/TSE.2008.88

Authors Biographies

Matjaž Drev, M.Sc. is an information security consultant at the National Institute of Public Health (NIJZ). Previously he worked as a State Supervisor for Personal Data Protection at Information Commissioner. He is one of the authors of Commentary on the GDPR. His professional interests are focused on information security, data privacy, and IT surveillance.

Dalibor Stanimirović, Ph.D. is a researcher and Head of Centre for Health Care Informatics at the National Institute of Public Health of the Republic of Slovenia (NIJZ). He is an Assistant Professor of informatics in public administration at the University of Ljubljana and a member of editorial boards of several international academic journals. His research work has been published in high-ranked scientific journals and presented at leading conferences and seminars. His general research interests include ICT policies and projects in health care, evaluation metrics and models, government enterprise architectures, and health information systems.

Boštjan Delak, Ph.D. is an Assistant Professor at the Faculty of Information Studies, in Novo mesto, Slovenia, where he teaches: Evaluation, Testing and Auditing of Information systems and Basics of Information Security. He is an active certified information system auditor. He has more than 40 years of experiences within information systems. He conducted more than 80 information systems due diligences and more than 150 information systems audits. His fields of interest are: information system due diligence, information system analysis, and knowledge management.