Drev M, Stanimirović D, Delak B, ‘Meta-analysis of privacy legal framework: revising the various approaches for balancing privacy risks and usability of healthcare information systems' (2024) 2 EJPLT, 221 – 232.
DOI: https://doi.org/10.57230/EJPLT242MDDSBD

EJPLT
ISSN 2704-8012

Meta-analysis of privacy legal framework: revising the various approaches for balancing privacy risks and usability of healthcare information systems

Meta-analisi del quadro normativo sulla privacy*: revisione dei differenti approcci per bilanciare i rischi per la privacy e l'usabilità dei sistemi informativi sanitari*

Matjaž Drev
Information security consultant, Ph.D., Center for Healthcare Informatics, National Institute of Public Health

Dalibor Stanimirović
Associate Professor, Ph.D., Faculty of Public Administration University of Ljubljana

Boštjan Delak
Assistant Professor, Ph.D., Faculty of information studies in Novo Mesto

Abstract

The integration of information and communication technologies with advanced machine learning, or artificial intelligence, brings both benefits and risks. These risks are particularly relevant in the context of personal data protection in healthcare, where non-compliance with legal requirements can lead to severe consequences for patients and substantial fines for healthcare institutions. A proactive approach to managing these risks involves the use of privacy by design frameworks and conceptual tools. This paper presents an overview of key privacy framework, highlighting their potential to deepen theoretical understanding and support the development of conceptual models that may enhance data protection in healthcare. Using qualitative and comparative research focused on content analysis, this study examines the role of these frameworks in embedding privacy principles within organizations. While primarily theoretical, the findings provide deeper insights into the principles underlying information privacy and lay a foundation for practical applications, such as testing frameworks through case studies to improve privacy compliance.

Abstract

L'integrazione delle tecnologie dell'informazione e della comunicazione con l'apprendimento automatico avanzato, o intelligenza artificiale, comporta vantaggi ma anche rischi. Tali rischi sono particolarmente rilevanti nel contesto della protezione dei dati personali in ambito sanitario, dove la mancata conformità ai requisiti normativi può portare a gravi conseguenze per i pazienti e a sanzioni elevate per le istituzioni sanitarie. Un approccio proattivo alla gestione di questi rischi prevede l'utilizzo di quadro normativo e strumenti concettuali di privacy by design. *Questo articolo presenta una panoramica del quadro normativo di riferimento per la* privacy, *evidenziando il suo potenziale per approfondire la comprensione teorica e sostiene lo sviluppo di modelli concettuali che possano migliorare la protezione dei dati in ambito sanitario. Utilizzando una ricerca qualitativa e comparativa incentrata sull'analisi dei contenuti, questo studio esamina il ruolo del* privacy framework *nel radicare i principi della* privacy *all'interno delle organizzazioni. Pur essendo principalmente teorici, i risultati forniscono approfondimenti sui principi alla base della* privacy *delle informazioni e gettano le basi per applicazioni pratiche, come la sperimentazione dei* framework, *attraverso casi di studio per migliorare la conformità alla* privacy.

Keywords: personal data; data protection; privacy by design; privacy frameworks; meta-analysis; healthcare information systems

Summary: 1. Introduction. – 2. Methods. – 2.1. Literature review. – 2.2. Comparing frameworks. – 2.3. Building a model. – 3. Results. – 4. Discussion. – 5. Conclusions.

1. Introduction

In contemporary society, increasing emphasis is placed on personal data protection.[1] This importance is an expression of respect for individual privacy and also a way to ensure compliance with legal requirements. Such compliance became particularly important in the European Union (EU) after the introduction of the General Data Protection Regulation (GDPR).[2] The USA has proposed American Data Privacy and Protection Act (ADPPA) which is still in legislative phase [3] ;however, an increasing number of states, for example, California, Virginia, Colorado, Connecticut, and Utah [4] have adopted information privacy laws.

One particular feature of GDPR is promoting the concept of privacy by design, which originates from Ann Cavoukian's influential essay.[5] The basic idea is to use different principles to shape the development and use of Information

[1] B Custers, G Malgieri, 'Priceless Data: Why the EU Fundamental Right to Data Protection is at Odds with Trade in Personal Data' (2022) 45 Comput Law Secur Rev 83.

[2] J Ruohonen, K Hjerppe, 'The GDPR Enforcement Fines at Glance' (2022) 106 Inf Syst 76.

[3] A Quay, 'Desperation for Legislation: The Need for the American Data Privacy and Protection Act' (2024) 41(4) Wis. Int'l L. J. 707.

[4] F Bellamy, 'U.S. Data Privacy Laws to Enter New Era in 2023' (2023) <https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/> accessed 16 May 2024.

[5] A Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (2009) https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 1 March 2024.

Communication Technology (ICT) in a way that interferes as little as possible with the privacy of individuals. However, Gurses, Troncoso, and Diaz[6] pointed out that the principles of privacy by design set by Cavoukian are vaguely defined and therefore unsuitable for use in developing frameworks and conceptual tools.

During our attempt to develop a conceptual model of privacy by design, which would be concise enough to use in case studies, we had to explore other approaches on how to implement privacy principles into the design and use of ICT. Through research, we found that substantial work has already been done. Recent developments worldwide in the misuse of personal data and unauthorized intrusions into information systems have heightened global awareness and intensified the debate around data protection.[7] These incidents underscore the critical importance of understanding and embedding privacy principles at every stage of information system development. As a result, data privacy is increasingly viewed as a foundational component rather than an afterthought, prompting organizations and policymakers alike to prioritize the integration of robust security protocols and privacy frameworks.[8] This shift encourages the adoption of privacy by design approaches and drives the development of frameworks that help ensure personal data is safeguarded against emerging threats and unauthorized access. It also became clear that efforts to develop privacy by design continue at an accelerated pace.[9,10]

Based on a meta-analysis of different approaches, we determined the building blocks for a conceptual model and successfully tested it on several case studies within the healthcare sector. Results were encouraging and were published in two articles.[11,12] However, this paper will not go into detail on how we developed the conceptual model but is rather a summary of extensive meta-analyses of different privacy frameworks that already exist. These frameworks provide a solid foundation for further developing the idea of privacy by design and conceptual tools that can put this idea into practice.

The paper is organized as follows. In the next section, we shortly review the literature and compare the frameworks with model presentation. Section three present the results, followed by discussion and concluding remarks.

[6] S Gürses, C Troncoso, C Diaz, 'Engineering Privacy by Design' (2011) <https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf> accessed 24 July 2024.

[7] JM Kizza, 'System Intrusion Detection and Prevention' in *Guide to Computer Network Security*, Texts in Computer Science (Springer, Cham, 2024).

[8] LL Dhirani and others, 'Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review' (2023) 23(3) Sensors, 1151.

[9] C Kurtz, M Semmann, T Böhmann, 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors' (AMCIS 2018 Proceedings, New Orleans, Louisiana, 2018).

[10] FH Semantha and others, 'A Systematic Literature Review on Privacy by Design in the Healthcare Sector' (2020) 9 Electronics 452.

[11] M Drev, B Delak, 'Conceptual Model of Privacy by Design' (2021) 62(5) J Comput Inf Syst 888.

[12] M Drev, D Stanimirović, B Delak, 'Implementation of Privacy by Design Model to an eHealth Information System' (2022) 10(1) Online J Appl Knowl Manag 77.

2. Methods.

2.1 Literature review.

Though the original concept of privacy by design is attributed to Ann Cavoukian`s essay "Privacy by Design: The 7 Foundational Principles",[13] which was published in the 1990s, the basic idea of implementing privacy concerns into existing and new ICT is even older. In the 1980s, authors such as Denning[14] and Chaum[15] wrote about concerns regarding the erosion of information privacy and ways to protect it through specific design of ICT. This approach later evolved into a privacy framework called “privacy enhancing technologies” (PETs).[16] Extensive meta-analyses of research work on privacy by design were made by Kurtz et al.[17] and Semantha et al.[18] In both studies authors examined how often the phrase “privacy by design” appeared in the titles, abstracts, or keywords of scientific articles. They reviewed the following databases: ACM Digital Library, AISeL, EBSCO Business Source Complete, EBSCO EconLit, IEEEXplore, ProQuest, CDU library, and ScienceDirect.

During the last two decades, different attempts were made to either build on the original idea of privacy by design or develop new approaches. Authors such as Spiekermann and Cranor,[19] Gurses et al.,[20] Hoepman,[21] Colesky et al.[22] and Nguyen & Tran,[23] focused on procedural aspects of information privacy protection. This was similar to the concept of “Privacy Impact Assessment” (PIA) which emphasized a project-based and systematic approach to the protection of personal data. PIA was mainly developed by Bennet,[24] Clarke,[25] Cavoukian[26] and De Hart and Papakonstantinou.[27] It also became part of the

[13] A Cavoukian, ‘Privacy by Design: The 7 Foundational Principles’ (n 4).

[14] DE Denning, *Cryptography and Data Security* (Addison-Wesley Publishing Company, Boston, USA, 1982).

[15] D Chaum, ‘Security without Identification Card Computers to Make Big Brother Obsolete’ (1985) 28 Commun ACM 1030.

[16] GM Garrido and others, ‘Revealing the Landscape of Privacy-Enhancing Technologies in the Context of Data Markets for the IoT: A Systematic Literature Review’ (2022) 207 J Netw Comput Appl, 103465.

[17] C Kurtz, M Semmann, T Böhmann, ‘Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors’ (n 7).

[18] FH Semantha and others, ‘A Systematic Literature Review on Privacy by Design in the Healthcare Sector’ (n 9).

[19] S Spiekermann, LF Cranor, ‘Engineering Privacy’ (2009) 35 IEEE Trans Softw Eng 67.

[20] S Gürses, C Troncoso, C Diaz, ‘Engineering Privacy by Design’ (n 5).

[21] JH Hoepman, ‘Privacy Design Strategies’ (2014) IFIP International Information Security Conference 446.

[22] M Colesky, JH Hoepman, C Hillen, ‘A Critical Analysis of Privacy Design Strategies’ (2016) Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops 33.

[23] MT Nguyen, MQ Tran, ‘Balancing Security and Privacy in the Digital Age: An In-Depth Analysis of Legal and Regulatory Frameworks Impacting Cybersecurity Practices’ (2023) 6(5) Int J Intell Autom Comput 87.

[24] C Bennett, *The Privacy Impact Assessment Handbook* (2007) https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/09/PIAhandbookV2.pdf accessed 2 February 2024.

[25] R Clarke, ‘Privacy Impact Assessment: Its Origins and Development’ (2009) 25 Comput Law Secur Rev 123.

[26] A Cavoukian, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers* (2011) <http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf> accessed 27 January 2024.

[27] P De Hert, V Papakonstantinou, ‘*Transparency in the European Data Protection Regulation: Implications for Privacy Impact Assessments’* (2016).

GDRP, albeit under the abbreviation Data Protection Impact Assessment (DPIA).[28]

With the rapid advancement of ICT, the increasing interconnectedness of information systems, and the rising need to address and prevent security risks, several alternative approaches have been explored. Hoepman[29] emphasized the importance of privacy protection strategies, distinguishing between data-oriented and process-oriented strategies. Foukia et al.[30] developed the privacy protection framework PISCES, Jensen et al.[31] developed STRAP, Kalloniatis et al.[32] developed PRIS, and Piras, L. et al.[33] developed DEFeND Architecture. The Federal Trade Commission developed Fair Information Practice Principles (FIPP) which are similar to GDPR's basic principles. The European Commission formed a consortium of 11 research institutions and started project PRIPARE. Within the project, review of existing privacy methods was done, and the result was the publication of the guidelines "PRIPARE Handbook - Privacy and Security by Design Methodology" which included practical instructions for ICT developers.[34]

Important contributions were made by the International Standard Organization (ISO) with the development of standards such as ISO/IEC 27701:2019 which translates GDPR provisions into a precise control list and ISO/IEC 29100:2011, which provides guidelines on how to implement PIA into data processing operations. In this context, standard ISO/IEC 27001:2022 should also be mentioned, as it provides a comprehensive information security control list. In the context of guidelines, in 2020 National Institute of Standards and Technology (NIST) issued "The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management".[35]

2.2 Comparing frameworks.

Through the meta-analysis of contributions made by previously listed authors, the main privacy by design frameworks were defined: GDPR, PET, PIA, FIPP, and Privacy Strategies. These frameworks were analyzed in more detail to compare their strengths and weaknesses (Table 1).

[28] G Georgiadis, G Poels, 'Towards a Privacy Impact Assessment Methodology to Support the Requirements of the General Data Protection Regulation in a Big Data Analytics Context: A Systematic Literature Review' (2022) 44 Comput Law Secur Rev 105640.

[29] JH Hoepman, 'Privacy Design Strategies' (n 20).

[30] N Foukia, D Billard, E Solana, 'PISCES: A Framework for Privacy by Design in IoT' in Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST) (2016, Auckland, New Zealand).

[31] C Jensen and others, 'STRAP: A Structured Analysis Framework for Privacy' https://www.academia.edu/62138420/Strap_A_structured_analysis_framework_for_privacy accessed 12 May 2024.

[32] C Kalloniatis, E Kavakli, S Gritzalis, 'Addressing Privacy Requirements in System Design: The PriS Method' (2008) 13 Requir Eng 241.

[33] L Piras and others, 'DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance' in Proceedings - 16th Trust, Privacy and Security in Digital Business International Conference 2019 (2019) 78.

[34] PRIPARE Project, *PRIPARE Handbook - Privacy and Security by Design Methodology* (2016) http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf accessed 7 May 2024.

[35] NIST, *The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (2020) https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf accessed 23 May 2024.

However, regarding the selection of frameworks, additional explanations should be added. The selection was to some extent guided by the requirements of the primary research project – the development of the privacy by design model. As this model was intended to be used by EU organizations for monitoring and improving compliance with European legal requirements, GDPR was chosen as a baseline. Although comparison of GDPR with other legal frameworks such as the ADPPA, California Consumer Privacy Act (CCPA), China's Personal Information Protection Law (PIPL)[36], Brazil's General Data Protection Law (LGPD), or Japan's Act on the Protection of Personal Information (APPI), would seem more appropriate and could offer new insights, comparative legal approach was not necessary for the primary purpose of developing the conceptual model. On the other hand, assessing if GDPR includes elements of other methodological approaches to privacy by design, was necessary.

Table 1: Comparison of privacy by design frameworks

	GDPR	PET	PIA	FIPP	Privacy Strategies
Characteristics	A binding legal document that organizations in the EU must comply with. It contains procedural and technical dimensions of personal data protection.	Recommendations for using IT in a way that ensures the least intrusion into privacy. Emphasis on anonymization, data obfuscation, and encryption techniques.	Recommendations for the design of personal data processing operations in such a way that the privacy of individuals is protected as comprehensively as possible. The focus is on procedural aspects of data protection. It includes the use of tools such as the decision tree and the data circle. It emphasizes the importance of risk analysis.	Recommendations that are followed primarily in the US, not in the EU. Very similar in content to GDPR, they mainly cover legal and to some extent organizational aspects, not much focus on security. Emphasis on the minimization of data processing, transparency, informing individuals, and protecting the right to choose.	Data oriented strategies are similar in content to the PET framework, which emphasizes detailed technical approaches to achieve anonymization, obfuscation, and encryption of data. Process oriented strategies, on the other hand, are similar to frameworks such as PIA and FIPP by emphasizing data control, the possibility of exercising data rights, and ensuring compliance.
Advantages	Applicable legal regulation. Violations are sanctioned by supervisory authorities. A comprehensive approach to the protection of personal data. Legal aspects of data protection are described in detail.	Strong focus on the technical aspect of data protection. A detailed description of IT methods for achieving data obfuscation.	Its recommendations are formally included in GDPR. A comprehensive, proactive, systematic, and transparent approach to the protection of personal data.	The framework is similar in content to GDPR, relatively comprehensive approach, an emphasis on legal and organizational dimensions of data protection. Focus is on the protection of the right individuals.	Data and process oriented strategies fully cover all aspects of personal data protection.
Weaknesses	The procedural aspects of data protection are not defined and described in detail. Security (technical) aspects of personal data protection are not defined and described in detail.	These are non-binding recommendations. The technical aspects of data protection are taken into account, but not much consideration is given to the legal and organizational dimensions.	There are no particular disadvantages, PIA as an approach is already included in the GDPR. The PIA itself is not binding, except in the segment covered by the GDPR.	This framework is general and less comprehensive than the GDPR, taking into account selected legal and organizational aspects, but not the technical aspects of personal data protection. FIPPs are less binding than GDPR, they apply mainly in the USA, not the EU.	These are partial and scattered approaches made by different authors, which are less coherent and condensed than, for example, the PIA framework. These approaches are not mandatory for organizations.

[36] PA Weber, N Zhang, H Wu, 'A comparative analysis of personal data protection regulations between the EU and China '(2020) 20 Electronic Commerce Research 565–587.

2.3 Building a model.

After reviewing and comparing the selected privacy frameworks, we had to choose one and use it for designing a conceptual model. As our effort was focused on providing tools for achieving compliance with GDPR requirements, that framework proved itself most suitable for our needs since the model was intended to be used primarily on EU organizations. Also, the approach that GDPR takes on data protection is relatively holistic[37], it takes into account both legal, organizational, and security aspects. Building upon the GDPR framework, it was necessary to determine individual building blocks that should make up the model. In this regard, a meta-analysis conducted by Huth and Matthes[38] proved most useful (Table 2). They reviewed research by Bellotti and Sellen,[39] Hong et al.,[40] Jensen et al.,[41] Kalloniatis et al.,[42] Spiekermann and Cranor,[43] Deng et al.,[44] Hoepman,[45] and Notario et al.[46] Their goal was to determine whether; by comparing different studies, it is possible to determine the general building blocks that define privacy by design.

Table 2: Presence of privacy by design elements in the contributions of selected authors.[47]

Analyzed paper / presence of privacy by design elements Legend: ● – element present ◐ – element partially present ○ – element not present	Pseudonymity	Unlinkability	Access control authorization	Integrity	Confidentiality	Accessibility	Data minimization	Transparency of processing	Storage limitation	Purpose limitation	Accountability	Encryption

[37] A Datoo, 'Data in the post-GDPR world' (2018) 9 Computer Fraud and Security 17–18.

[38] D Huth, F Matthes, 'Appropriate Technical and Organizational Measures: Identifying Privacy Engineering Approaches to Meet GDPR Requirements' (2019) AMCIS 2019 Proceedings 1790.

[39] V Bellotti, A Sellen, 'Design for Privacy in Ubiquitous Computing Environments' in Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW '93 (1993) 77 https://doi.org/10.1007/978-94-011-2094-4_6 accessed 2 May 2024.

[40] J Hong and others, 'Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems' (2004) Proceedings of the 2004 Conference on Designing Interactive Systems Processes, Practices, Methods, and Techniques - DIS '04 91 <https://doi.org/10.1145/1013115.1013129> accessed 11 January 2024.

[41] C Jensen and others, 'STRAP: A Structured Analysis Framework for Privacy' (n 30).

[42] C Kalloniatis, E Kavakli, S Gritzalis, 'Addressing Privacy Requirements in System Design: The PriS Method' (n 31).

[43] S Spiekermann, LF Cranor, 'Engineering Privacy' (n 18).

[44] M Deng and others, 'A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements' (2011) 16 Requir Eng 3.

[45] JH Hoepman, 'Privacy Design Strategies' (n 20).

[46] N Notario and others, 'PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology' in Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015 (2015) 151.

[47] D Huth, F Matthes, 'Appropriate Technical and Organizational Measures: Identifying Privacy Engineering Approaches to Meet GDPR Requirements' (n 35).

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	○	○	○	●	●	●	●	●	●	●	●	◐

The findings of a comparative analysis conducted by Huth and Matthes[48] suggest a certain universality of privacy by design elements, which is encouraging for any effort to create a model that is general enough to be used in a variety of personal data processing contexts and specific enough to be introduced into personal data processing operations within a reasonable time frame.

3. Results.

In our effort to design a conceptual model, we attempted to connect basic principles of privacy by design as set by Ann Cavoukian[49] with the GDPR privacy framework and the set of building blocks identified as common across different approaches by Huth and Matthes (Table 3).[50]

Table 3: Comparison of three approaches to understanding privacy by design.[51]

Basic principles (Ann Cavoukian, 2009)	**GDPR framework**	**Comparative analysis (Huth and Matthes, 2019)**
Proactivity	DPIA	/
Privacy as default	Basic principles of the GDPR (Article 5)	Transparency of processing, minimum scope of processing, limitation of data retention, limitation of the purpose of processing
Privacy built into the design of the solution	Default and built-in data protection (Article 25)	Pseudonymization, non-connectivity, minimum scope of processing, limitation of data retention, limitation of purpose of processing, liability
Full functionality	/	/
Data security throughout the entire processing cycle	Security of personal data (Article 32)	Access control, integrity, confidentiality, availability, encryption.

[48] Ibid.

[49] A Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (n 4).

[50] D Huth, F Matthes, 'Appropriate Technical and Organizational Measures: Identifying Privacy Engineering Approaches to Meet GDPR Requirements' (n 35).

[51] M Drev, B Delak, 'Conceptual Model of Privacy by Design' (n 10).

Transparency	Basic principles of the GDPR (Article 5), legality of processing (Article 6), notification of individuals (Article 12).	Processing transparency, responsibility.
Respect for the individual	Informing individuals (Article 12), rights of individuals (Articles 15, 16, 17, 18, 20, 21).	Processing transparency, responsibility

From the comparison table, it can be seen that the basic building blocks of privacy by design (except "full functionality") are present in all presented approaches (Table 3). A conceptual model of privacy by design could therefore be designed with the help of building blocks from any approach or with a combination of different approaches. However, when combining approaches, care must be taken to preserve elements from the same lines, as these refer to related concepts in terms of content, and it is also reasonable to determine the basic starting point, as there may be terminological ambiguities, duplication and the introduction of unnecessary complexity into model.

Elements from the GDPR framework were identified and used as building blocks for the conceptual model of privacy by design (Figure 1). They were grouped into one of three sets: "legal elements", "security elements", and "privacy by design and by default elements".[52] The sets are consistent with the structure of GDPR where legal elements occupy a central position, followed by data security, and finally by privacy by design and by default provisions.

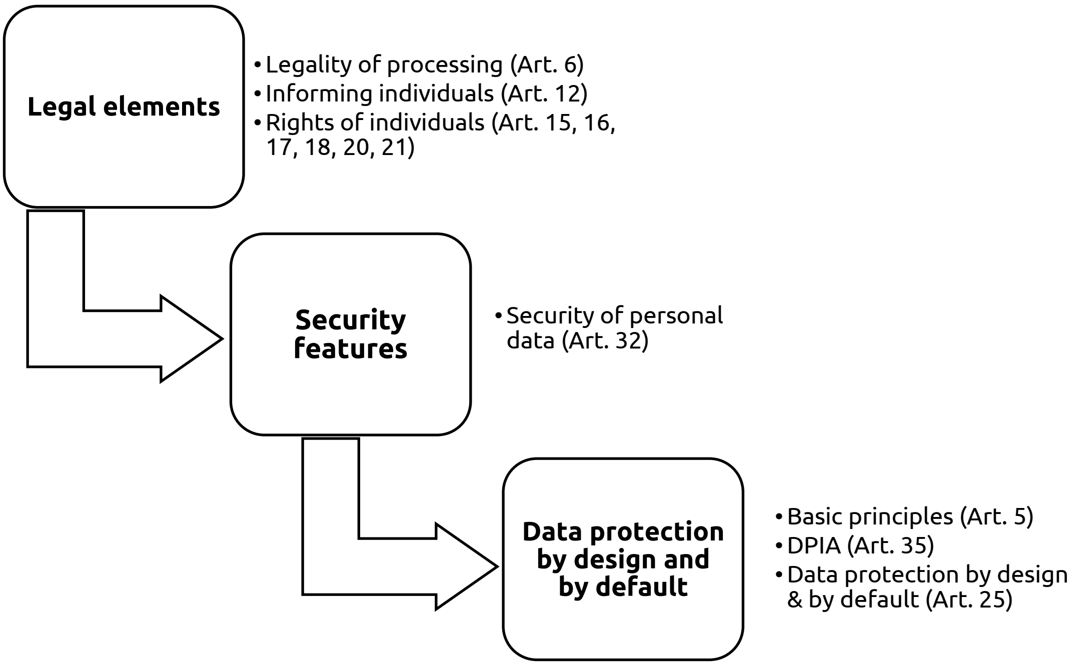
Legal elements
• Legality of processing (Art. 6)
• Informing individuals (Art. 12)
• Rights of individuals (Art. 15, 16, 17, 18, 20, 21)
Security features
• Security of personal data (Art. 32)
Data protection by design and by default
• Basic principles (Art. 5)
• DPIA (Art. 35)
• Data protection by design & by default (Art. 25)

Figure 1: Representation of the conceptual model of privacy by design.[53]

[52] Ibid.

[53] Ibid.

The described conceptual model was tested on the Slovenian central health information system (eHealth) in 2021.[54] Two years later, the model was tested on three additional healthcare organizations, however, the results have not yet been published.

4. Discussion.

The fundamental question—whether one privacy by design framework offers noticeable advantages over others—remains unresolved. Currently, the available data is insufficient to provide a definitive answer. The comparison made in this article was theoretically oriented, however, the challenge of finding out if the specific framework is more effective in promoting theoretical understanding or providing the development of conceptual tools is beyond the scope of this article. This assessment may present a considerable test for future research attempts in the field.[55] It will require tackling difficult questions such as how to evaluate the effectiveness, how to compare different frameworks and models, and how to isolate the analyzed personal data processing operations in a way that will allow testing of different models without the intervention of one interfering with and skewing the results of another.[56] As the theoretical foundations of some of the privacy frameworks vary widely and are substantially different, it would be appropriate to compare those frameworks that display sufficient similarities in content and structure. Evaluation criteria could be developed using established standards, for example, ISO/IEC 27701 which deals with personal data protection.[57] Such a set of criteria could form the basis for a comprehensive assessment tool that can objectively measure each framework's proficiency. Case studies would then have to include organizations with comparable data processing complexities. Focusing on similar organizations could help control variables and improve the reliability of comparisons.

Regarding the work done with the conceptual model that was derived from the GDPR framework, the results are favorable for the time being. It seems that the model provides an appropriate compromise between generality and specificity.[58] However, one challenge lies in ensuring diversity within these studies. Namely, all four studies were made on organizations in the healthcare sector in one EU member state, therefore substantially different circumstances could open new dilemmas and show different results.[59] While promising, these findings may not extend to other areas or organizations with different levels of

[54] M Drev, D Stanimirović, B Delak, 'Implementation of Privacy by Design Model to an eHealth Information System' (n 11).

[55] O Ayalon, E Toch, 'User-centered privacy-by-design: Evaluating the appropriateness of design prototypes' (2021) 154 Int J Hum Comput Stud 102641.

[56] F Bu and others, '"Privacy by Design" implementation: Information system engineers' perspective' (2020) 53 Int J Inf Manage 102124.

[57] L Carmichael, W Hall, M Boniface, 'Personal data store ecosystems in health and social care' (2024) 12 Front Public Health 1348044.

[58] S Mohanty, 'Security and Privacy by Design is Key in the Internet of Everything (IoE) Era' (2020) 9(2) IEEE Consumer Electron Mag 4–5.

[59] A Carboni and others, 'Privacy by design in systems for assisted living, personalised care, and wellbeing: A stakeholder analysis' (2023) 4 Front Digit Health 934609.

data-processing complexity. Important consideration in evaluating privacy by design frameworks is the varying impact of sector-specific regulatory and operational requirements.[60] Different industries have unique data protection challenges and requirements, which can influence the relevance and effectiveness of specific privacy frameworks. For instance, healthcare organizations must adhere to strict data privacy standards due to the sensitive nature of health information, while financial institutions may focus more on data security due to the risk of financial fraud.[61] Understanding the sector-specific impact of privacy frameworks is essential for determining whether one framework is better suited for a particular type of organization over another. Therefore, future research should include a comparative study of privacy frameworks across sectors with distinct data handling conditions, regulatory requirements, and personal data processing complexities. This would reveal the adaptability and effectiveness of different privacy by design models in addressing diverse compliance landscapes and operational demands. Such research could also help organizations in specific sectors identify frameworks that best align with their privacy obligations and security goals.[62] Adding organizations from non-EU countries would also add to the diversity of the testing environment and in perspective enable higher robustness of the conceptual model. Such an expansion of the model could reveal different sector-specific challenges and insights that remain hidden within a single industry or region.[63] A promising venue for further research in this context would be comparing GDPR with other personal data protection Acts, most notably the Health Insurance Portability and Accountability Act (HIPPA)[64] and ADDPA.

In the long term, however, automated implementations—potentially through AI-based tools—could streamline the evaluation and integration of privacy frameworks across organizations. AI-driven analysis and automation could simplify the application of privacy by design principles, potentially offering solutions for real-time compliance and adaptive privacy strategies.

A successful implementation of any privacy by design framework hinges on effective stakeholder engagement, particularly from those responsible for data handling and privacy compliance within an organization.[65] Different frameworks may vary in how they encourage stakeholder involvement, training, and accountability, all of which are critical for effective privacy management. Therefore, future studies should evaluate how well various frameworks support stakeholder engagement and facilitate privacy-conscious

[60] L Iwaya and others, 'On the privacy of mental health apps: An empirical investigation and its implications for app development' (2023) 28(1) Empir Softw Eng 2.

[61] A Tewari, 'mHealth Systems Need a Privacy-by-Design Approach: Commentary on "Federated Machine Learning, Privacy-Enhancing Technologies, and Data Protection Laws in Medical Research: Scoping Review"' (2023) 25 J Med Internet Res e46700.

[62] A Aljeraisy, M Barati, O Rana, C Perera, 'Privacy laws and privacy by design schemes for the internet of things: A developer's perspective' (2021) 54(5) ACM Computing Surveys (Csur) 1–38.

[63] E Schultes, M Roos, LO Bonino da Silva Santos, G Guizzardi, J Bouwman, T Hankemeier, A Baak, B Mons, 'FAIR Digital Twins for Data-Intensive Research' (2022) 5 Front Big Data 883341.

[64] A Oakley 'HIPAA, HIPPA, or HIPPO: What Really Is the Heath Insurance Portability and Accountability Act? ' (2023) 42(6) Biotechnology Law Report.

[65] L Alkhariji and others, 'Semantics-based privacy by design for Internet of Things applications' (2023) 138 Future Gener Comput Syst 280–295.

organizational cultures. For example, frameworks that mandate regular training, clear reporting channels, and contractual as well as accountability mechanisms may foster a stronger privacy culture than those lacking such requirements.[66] Additionally, engaging stakeholders early and often in the framework selection and implementation processes can ensure that privacy practices align with organizational values and practical needs.[67] This emphasis on stakeholder engagement can also influence the framework's long-term sustainability, as continuous involvement and feedback help refine privacy practices. Future studies could investigate the degree to which stakeholder engagement influences the overall effectiveness of privacy frameworks, which would provide valuable insights into best practices for fostering organizational commitment to privacy by design principles.

5. Conclusions.

From its origins in the 1990s, the idea of privacy by design has seen notable expansion. In addition to academic interest, it became part of the most comprehensive legal document for the protection of personal data – GDPR. Because of the increasing influence of ICT, (re)thinking privacy is becoming increasingly interesting for organizational and information science. With increasing risks of cybersecurity threats, integrating privacy measures such as data minimization, pseudonymization, and encryption, should also benefit the resilience of information systems without sacrificing general usability. Authors offered different frameworks for understanding privacy by design. A comparison of these approaches shows that commonalities are much more prevalent than differences. Such commonalities can be used to form common grounds for new ventures: from a deeper understanding of privacy to the development of conceptual tools and models which could even be integrated with artificial intelligence interfaces for more efficient (semi)automated implementation.

[66] E Tosi, 'Dati personali e contratto: un ossimoro apparente' (2023) 2 EJPLT 71–92.
[67] R Raab and others, 'Federated electronic health records for the European Health Data Space' (2023) 5(11) Lancet Digit Health e840–e847.