Integrating Privacy-By-Design with Business Process Redesign

Vasiliki Diamantopoulou(✉) and Maria Karyda

Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece
{vdiamant,mka}@aegean.gr

Abstract. Among the numerous challenges that organisations face, information security is undoubtedly an important concern, and as of lately, compliance with personal data regulation (e.g., the General Data Protection Regulation – GDPR in the EU) is a necessity, while requirements for privacy-by-design need also to be met. This paper proposes a comprehensive method to support the identification, modelling, (re)design, implementation, and realisation of privacy aware/compliant business processes, in order to incorporate personal data protection principles into all work practices and business processes in an organisation. More specifically, this method integrates the main steps of a Data Protection Impact Assessment into business process management, to ensure the identification of personal data flow throughout the organisation and support the assessment of privacy-related risks and enhance personal data protection.

Keywords: Business process redesign · Data protection impact assessment · Privacy-by-design · Privacy patterns

1 Introduction

Information and Communication Technologies (ICT) play a significant role in every-day life, providing users with personalised services that require or collect their personal information. Personal data has become a main asset for modern enterprises and is exchanged on a broad scale (Spiekermann et al. 2015) as it is considered the basis for developing, interacting, and decision making. The necessity of protecting individuals' personal data is of utmost importance, especially when taking under consideration the value that personal data has for the digital economies and the interest that its collection attracts, either for public or private organisations. This necessity has been also imposed by legal and contractual obligations, and since May 2018, is also imposed by the European Union's General Data Protection Regulation (GDPR) (European Parliament 2016). The protection of personal data has seen a major upheaval during the last decades, attracting the attention of politicians, developers, public and private organisations, legislators, authorities, as well as the general public. However, privacy preservation is not a straightforward process, as privacy is a multifaceted concept with various parameters that need to be taken into account, at technical and social level and are often determined by the inner

© Springer Nature Switzerland AG 2022
S. Katsikas et al. (Eds.): ESORICS 2021 Workshops, LNCS 13106, pp. 127–137, 2022.
https://doi.org/10.1007/978-3-030-95484-0_8

and outer context of organisations. Since GDPR came into force, several reports have identified that organisations are still not fully aware of the GDPR's potential impact, e.g., (Reuters 2019) and that they are not fully ready to accommodate GDPR compliance issues. In a recent survey (IAAP-FTI 2020) which was published in 2020 by the International Association of Privacy Professionals, less than half of respondents (47%) answered that they are fully compliant with the GDPR. Reported challenges for GDPR compliance (McKinsey and Company 2019) include the exercising of the rights from the data subjects (GDPR, Articles 12–22), the automation of the records of processing activities (GDPR, Article 30) and the efficiency of the designed business processes during the preparations for the GDPR.

Complying with GDPR is a demanding process for all organisations, requiring various competences from different areas of expertise, including legal and technical, such as the information and communication systems security and privacy requirements engineering domain, as well as in depth knowledge of how different business units' function and, more importantly, the flow of personal information through the organisation. It is therefore important that organisations are supported throughout all tasks involved in fulfilling the GDPR requirements, considering the context, functions and the characteristics of each organisation. The provision of products and systems following privacy-by-design principles (European Data Protection Board 2019), as well as the adoption of business processes that respect data protection principles, can result to several intangible benefits for an organisation, including good reputation, improving trust in customer and business partners relationships (e.g., data processors, third parties, suppliers), by rendering organisations trustworthy and accountable, while these benefits, in a long term can also return tangible benefits, such as increase of profits. Both in the literature (i.e. Langheinrich 2001; Cavoukian 2009) and in accordance with the Article 25 of the GPDR, it is found that privacy-by-design principles should be applied *at the time of the determination of the means for processing and at the time of the processing itself*, to responsibly manage and to effectively protect the personal data processed by an organisation.

In existing approaches (Pullonen et al. 2017; Ahmadian et al. 2018; Tom 2018), it is not easy to follow the flow of information throughout the organisation's business processes, especially when examining it from a privacy perspective, taking personal data within these flows under consideration. Current approaches have mainly relied on the empirical capabilities of the analyst to pinpoint personal data and all related interconnections within business flows. This paper aims to contribute to addressing this challenge by proposing a method that supports personal data protection throughout the entire life cycle of the information within an organisation, focusing on business processes to identify and assess information flows in terms of their privacy impact, so as to ensure the basic requirements of privacy-by-design. The proposed method bridges the gap between business and privacy analysts so as to leverage privacy aware work practices throughout the organisation, improving data protection and raising a privacy aware culture in its members.

The rest of this paper is structured as follows: Sect. 2 presents the background analysis with respect to the components of the proposed method, while Sect. 3 describes the proposed method for integrating business process redesign and Data Protection Impact Assessment (DPIA) in the context of an organisation. In Sect. 4 we further discuss the

main pillars of the proposed method as well as the positive impact that its applicability will bring. Finally, in Sect. 5 we conclude the paper by raising issues for further practical research.

2 Background Analysis

Conduction of DPIA is a useful tool for the protection of personal data, and also comprises a requirement of the GDPR (GDPR/Article 35). DPIA supports (among others) organisations to gain the public's trust and confidence that privacy has been built into the design of a process, information system or programme. Conducting a DPIA, according to the GDPR, is mandatory when high-risk for the data subjects' rights is introduced by the processing of their data (e.g., when special categories of personal data are processed or when processing involves systematic evaluation of personal aspects or scoring). However, conducting a DPIA also comprises a good practice for data protection, and as the Article 29 Data Protection Working Party (2017) proposes, the organisations that process personal data should conduct DPIA in order to identify and reduce the privacy risks of the activities that process personal data and they are responsible for. Taking into account the high amount of personal data processed by several everyday applications, such as location-based services and fitness/well-being applications, conducting a DPIA emerges as a necessity in most cases of digital services provided to individuals. At the same time, the need for conducting a DPIA is also eminent in cases where extensive personal data collection is imposed by special circumstances, as for instance when the Covid19 lockdown rendered teleworking, telecommunication, and tele-education applications essential for society to continue operating, thus making necessary the extensive use of applications gathering data on the history of user interactions and metadata about their devices. In the same context, several applications have emerged for tracing people's contacts via their location data, found on their cell phone[1], to prevent the spread of the virus.

Taking into consideration the general philosophy of the GDPR, all organisations processing personal data should protect personal data throughout their entire lifecycle, in a holistic and context-aware manner (Henriksen-Bulmer et al. 2020), from their generation/insertion into the organisation till their disposal. This necessity applies not only to data that is preserved and processed via digital infrastructure, but also to personal data kept in hardcopy form. Data protection principles should be followed as a universal requirement for the whole organisation's scope. Privacy-by-design is an approach that requires the integration of key protection parameters by the organisation who is responsible for the processing of individuals' personal data into existing wider project management approaches. GDPR provisions facilitate to this direction by requiring companies, organisations, etc. to ensure that the protection of users' privacy is a basic parameter in the early stages of each project and then throughout its life cycle (Langheinrich 2001; Cavoukian 2009).

However, security and privacy requirements elicitation and the assessment of privacy risk that is imposed by a specific process or information system is not an easy task

[1] https://www.europarl.europa.eu/news/en/press-room/20200512IPR78915/covid-19-tracing-apps-meps-stress-the-need-to-preserve-citizens-privacy.

and security and privacy analysts are not always able to follow the flow of information throughout an organisation's business processes. It is necessary to consider all related business functions, as well as the inner and outer context of an organisation in order to assess the impact of the realisation of a privacy threat at any given point within any business process flow. Conducting a DPIA process, up to now, has mainly relied on the insight of analysts, in order to identify the information flows' interconnections, or it has relied on the repetition of this process for each critical flow. As security and privacy analysis is necessary for organisations that processes personal data, security/privacy requirements methodologies are implemented (indicatively, Kalloniatis et al. 2009; Mellado et al. 2010; Beckers 2012) aiming at evaluating the critical assets of an organisation. These methodologies support security/privacy experts to identify the requirements for the protection of an asset and to analyse the identified threats and vulnerabilities of an organisation.

Available methodologies/tools so far do not support the capturing of the flows of information in conjunction with the corresponding assets and the responsible entity for each process, and there is no connection and association of a system's security and privacy analysis with an organisation's hierarchical roles. The method described in the next section aims at addressing this gap, by integrating the main steps of a DPIA with the business process management, so as to facilitate the identification of personal data flow throughout the organisation, support the assessment of privacy related risks and enhance personal data protection.

The proposed method aims at supporting business processes management and/or (re)design of an organisation to support personal data protection. To achieve this, we draw on the frameworks and tools supporting the (re)design of business processes, i.e. Business Process Management (BPM) (Hammer 2015) disciplines, focusing on the modelling, analysis, and improvement of business processes in terms of efficiency and effectiveness. BPM tools allow analysts to capture the existing business processes within an organisation, including the infrastructure, i.e. the corresponding Information Systems (IS) being used, the involved roles for each process, the documents that each IS uses, produces, stores, etc., the retention period of each document, the origin (source) of each document as well as its final destination. Business process modelling tools can also support the identification of data flows within an organisation. Though the usefulness of BPM tools and methods has been acknowledged by the information security research community in providing comprehensive security for information assets (Kokolakis et al. 2000; Backes et al. 2003; Argyropoulos et al. 2017), such efforts can support the protection of personal information only partially and at a limited level (Diamantopoulou et al. 2017a). Limitations of current approaches also include that the notation of the personal data (and the special categories of personal data, i.e. sensitive data) is not supported, and that the criticality of the IS cannot be prioritised either. For example, in order to prevent data losses in a potential data breach, an organisation must have fortified the IS that stores the personal data rather than e.g., an IS responsible for the daily transaction of an e-commerce web service – that does not process personal data.

3 A Method for Integrating DPIA and Business Process Management

Our proposed method supports the identification, modelling, redesign, implementation, and realisation of security and privacy aware/compliant business processes, by identifying security and privacy risks to personal information flows for all business processes, and by employing privacy strategies for realising privacy preserving workflows. Figure 1 presents the steps of the proposed method.

The method follows the logic of a typical BPM approach that allows to capture, analyse, and model, in a systematic way, the organisation's business processes and workflows. Identification and analysis of business processes and information flows provides the basis for conducting a security and privacy requirements analysis, allowing the adoption of a business process perspective, which takes into account all involved roles, internal and external. This process provides an identification of information flows to be evaluated in terms of the basic data protection principles (i.e. data minimisation, accuracy, storage limitation, integrity and confidentiality, lawfulness, fairness and transparency, and purpose limitation) and to assess existing threats and vulnerabilities and identify security and privacy requirements. The proposed method also includes a DPIA process as an optional step. Organisations however are encouraged to conduct DPIA in the activities they perform that process personal data as they can also achieve benefits from the increased trust gained by their clients and collaborators which results from increased data protection.

The output of the analysis provides insights for managing (an, if needed, redesigning) business processes in a more efficient, secure and privacy-aware manner. To (re)design privacy-aware business processes different tools can be used, such as for example privacy process patterns (Diamantopoulou et al. 2017a, b) that will facilitate the analyst to associate privacy requirements with appropriate Privacy Enhancing Technologies (PETs). Privacy patterns can be applied to satisfy the identified privacy requirements, as they allow the capturing and sharing design knowledge (Alexander 1997; Borchers 2000) and encapsulate expert knowledge of PETs implementation at the operational level. Different types of privacy patterns are available (Kalloniatis et al. 2008) including i) administrative tools, ii) information tools, iii) anonymizer products, iv) services and architectures, v) pseudonymizer tools, vi) track and evident erasers, and vii) encryption tools. Each category contains specific technical implementation techniques which can be used as a basis for the designer along with the stakeholders and/or the organisation's developer team to decide and propose the most appropriate ones that will satisfy the identified privacy requirements.

The proposed method includes a repetitive process in accordance with the continuous improvement concept suggested by ISO/IEC 27001:2013 standard (2013) and the GDPR. This repetitive phase is also mandated by the fact that business processes may change within an organisation, and/or new Information Systems may be deployed.

The steps/phases of the proposed method are four. As we mentioned above, conducting a DPIA is not obligatory, however, organisations are encouraged to conduct it for

Fig. 1. Method for integrating privacy-by-design into business processes/workflows

new projects, products, or services. Below, we explain the main phases of the method, focusing on the main activities:

Analysis of Business Process and Identification of Personal Data: Main activities in this step include the capturing, identification, modelling and analysis of the organisation's business processes and workflows, along with the relevant information flows and it will also support the identification of related entities and stakeholders such as the responsible entity for the execution of such processes (internal entities of the organisation or external parties), the IS involved in each processing, the documents requested for each process, the flow of each document, and the responsible hierarchical roles for the execution of business processes. As existing BPM solutions lack characterisation and distinction of "personal data" or "sensitive data" we propose the inclusion of both of these object types in the design process using relevant annotations/metadata. To use the relevant annotations/metadata, analysts will draw on the descriptions and provisions in Article 30 of the GDPR about "records of processing activities".

Security and Privacy Analysis: Designing and implementing systems and/or services with respect to security and privacy requires the integration of security and privacy requirements into the typical engineering activities. In this step all critical assets are assessed, as well as the processes and flows of the previous steps, from a security and privacy perspective. More specifically, this step contains the identification of the critical assets of the organisation's business processes that affect the processing of personal data, potential threats that might have an impact on these assets and any vulnerabilities that these assets may have. Additionally, in this step, the interconnections between the corresponding lanes of the under-examination business processes reveal any associations between assets, as well as the impact of threats to all critical assets. By following this method, we are able to capture the impact of threats on any specific asset by examining it throughout its whole lifecycle and flow in the various business information processes. Finally, this step includes the documentation of existing security and privacy mechanisms and the analysis of a security and privacy assessment of all workflows and corresponding

assets entailing personal information, considering all security and privacy requirements affecting actors, assets, information, roles, and hierarchies.

DPIA Process (Optional): The objective of this step is the assessment of the privacy risk that can be materialised by the data processing activities carried out by the organisation and could have an impact on the privacy of the persons whose personal data is processed. Here, the analyst identifies the processing activities that may be either implemented directly by the organisation who is responsible for the data processing or by the organisation who is directly conducting the processing. The risk of each processing activity is analysed to the severity and the likelihood for a threat to have an impact on the data subject, while mitigation measures are identified in terms of applicable privacy patterns. This step takes as input the outcomes of the first two steps ((i) Analysis of business process and Identification of personal data and (ii) Security and Privacy analysis) and the appropriate (per case) privacy process patterns to guide selection and implementation of mitigation measures.

Redesign/Enhance Business Processes: Drawing on BPM concepts, the fourth step aims at the redesign of the business processes of the organisation, taking into account the results of the previous three components and employing privacy preserving patterns. The analyst uses the identified (from the second step) security and privacy requirements in order to construct robust and privacy preserving business processes, thus implementing privacy-by-design principles, impacting all the organisational processes. Analysts implement selected appropriate PETs for satisfying the requested security and privacy requirements. Through the redesign of the business processes and information flows the organisation will be enhancing their activities, leveraging the data protection principles in any node of this system, either systemic or human one.

Concluding, this method supports the aggregation of all the information and modelling analysis of business processes with data protection, supporting the privacy-by-design principles with the identified (security and) privacy requirements and by associating the privacy process patterns with the corresponding privacy requirements (as they have been identified in the second step).

4 Discussion

Up to now, and to the best of our knowledge, there is no comprehensive approach supporting organisations to manage the flow of personal information through their business processes that supports the need of organisation to comply with data protection legislation and follow the privacy-by-design principles. The proposed method draws on the concepts of business process management data protection to provide a method to enable organisations model and redesign their business processes in a privacy-aware context, establishing, thus, secure and privacy-aware business processes and delivering secure products/services, following privacy-by-design principles. Our approach allows organisations develop privacy preserving business practices and workflows, resulting in products and services that comply with data protection rules and requirements. In doing so, personal data protection practices and principles are leveraged into all organisational functions. Furthermore, the proposed method guides organisations to perform important

tasks with regard to GDPR compliance and provide concrete and detailed work practices and solutions, in the form of privacy patterns. More specifically, the proposed method aims has the following characteristics:

- **Provides comprehensive steps for privacy analysis:** This method supports the modelling, redesign, implementation and realisation of privacy aware/compliant business processes, by a) considering personal and sensitive data in the activity of business process capturing and modelling, b) identifying the responsible roles and associating them with the corresponding business processes, c) analysing business processes from a security and privacy perspective, d) assessing privacy risks to personal information flows of all business processes, and e) employing privacy preserving strategies for realising the respective workflows, utilising existing technologies, frameworks, methods and tools.
- **Supports GDPR compliant services and products:** The proposed method can help redesign an organisation's processes or products/systems they deliver to ensure they are GDPR compliant. This approach supports, from a business process handling perspective, a basic goal of the GDPR, Privacy-by-Design, meaning protecting personal data – from their data entry/acquisition/generation to their disposal. The proposed method also guides the business/privacy analyst in application of the privacy-by-design principles from a technical perspective (by identifying security/privacy requirements and mapping them to privacy patterns) and a business perspective (managing stakeholders involved in each step of the business process). Also, by following our structured approach and documenting each step of the (re)design process, organisations are assisted in demonstrating how they implemented GDPR requirements (accountability requirement of the data controller).
- **Provides Liability:** With the identification of the roles in the recorded business processes, the proposed method facilitates the identification of the key stakeholders involved in the business process steps and the roles involved in the DPIA. As a result, this method provides the analyst with insights to understand which person/role is responsible (or should be consulted) in the context of the analysis and who should be assigned the responsibility for implementation of the proposed changes in the business process (including the implementation of privacy/security measures). This type of guidance enhances the organisations' approach towards compliance, by identifying responsible and accountable entities for the implementation of BPR outcome. It is useful in cases of complex system processes running through different units of the organisation, where stakeholders are unwilling to take ownership for a process, and in cases of complex environments between partners, especially in cases of joint controllership or controller-processor relationships.
- **Utilises privacy patterns:** Privacy patterns assist developers to understand, in a better and more specific way, how to implement the various privacy properties and are considered as a more robust way for bridging the gap between the design and the implementation phase of a system or module of it. Their incorporation within the proposed method facilitates the analyst to associate the privacy requirements with the appropriate PETs.

- **Utilises and extends existing approaches:** The proposed method draws upon existing well-established concepts and approaches, extending them to develop a comprehensive approach that leverages data protection in all business processes and incorporates privacy preserving principles in services, products and projects developed. The familiarisation of the business analysts/security/privacy experts with the basic structure of each component will benefit the design process.
- **Leverages privacy-by-design principles and practices:** With the use of the various different approaches, we are able to redesign the system-based processes as well as the human-based processes. To this end, the organisation is able to demonstrate both the technical and the organisational measures they had apply to protect the personal data they process, satisfying, thus, the GDPR requirement for the accountability as well as for the protection of such data.

5 Conclusions

In this paper we have identified the difficulties that organisations face in their attempt to design their business processes so that they are efficient and effective while at the same time, protecting personal data that is being processed, respecting the core requirements imposed by relevant regulations, such as the GDPR, and follow, the privacy-by-design principles. To satisfy these challenges, in this work we propose a method that supports the identification, modelling, redesign, implementation, and realisation of privacy aware/compliant business processes, by identifying privacy risks to personal information flows for all business processes, and by employing privacy strategies for realising privacy preserving workflows. The core idea of the proposed method is that it draws upon existing well-established concepts and approaches, extending them to develop a comprehensive approach that leverages data protection in all business processes and incorporates privacy preserving principles in services, products and projects developed, filling in an important gap in data protection in organisations and assisting them with GDPR compliance.

The proposed method, up to now, has not been validated in a real-life case scenario, but we intend to do so, as part of our future research goals, which also include the following: we aim to extend existing privacy patterns and develop a tool that includes an inventory of privacy patterns that can assist analysts in selecting, developing, managing and implementing them.

Future directions of this work also include the development of a tool that supports the implementation of the proposed method. This tool will provide a combination of BPM modelling functionalities, integrate the privacy patterns inventory, support security and privacy analysis conducting, and DPIA conducting, so that organisations can model and redesign their business processes following a data protection perspective, incorporating privacy-by-design principles, and achieving an end-to-end data protection process within their information flows and their workflows.

Additionally, we intend to provide a validation process to support the proposed method. The validation process will be based on the analysis of a case study approach that will allow us to better examine the steps of each phase of this method.

References

Ahmadian, A.S., Strüber, D., Riediger, V., Jürjens, J.: Supporting privacy impact assessment by model-based privacy analysis. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, pp. 1467–1474 (2018)

Alexander, C.: A Pattern Language: Towns, Buildings, Construction. Oxford University Press, Oxford (1977)

Argyropoulos, N., Mouratidis, H., Fish, A.: Supporting secure business process design via security process patterns. In: Enterprise Business-Process and Information Systems Modeling, pp. 19–33. Springer, Cham (2017)

Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017). https://ec.europa.eu/newsroom/document.cfm?doc_id=47711. Accessed 19 Apr 2021

Backes, M., Pfitzmann, B., Waidner, M.: Security in business process engineering. In: van der Aalst, W.M.P., Weske, M. (eds.) BPM 2003. LNCS, vol. 2678, pp. 168–183. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-44895-0_12

Beckers, K.: Comparing privacy requirements engineering approaches. In: 2012 Seventh International Conference on Availability, Reliability and Security, pp. 574–581. IEEE (2012)

Borchers, J.O.: A pattern approach to interaction design. In: Proceedings of the 3rd Conference on Designing Interactive Systems: Processes, Practices, Methods and Techniques, pp. 369–378. ACM (2000)

Cavoukian, A.: Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada 5 (2009)

Diamantopoulou, V., Argyropoulos, N., Kalloniatis, C., Gritzalis, S.: Supporting the design of privacy-aware business processes via privacy process patterns. In: 2017 11th International Conference on Research Challenges in Information Science (RCIS), pp. 187–198. IEEE (2017a)

Diamantopoulou, V., Kalloniatis, C., Gritzalis, S., Mouratidis, H.: Supporting privacy by design using privacy process patterns. In: De Capitani di Vimercati, S., Martinelli, F. (eds.) SEC 2017. IAICT, vol. 502, pp. 491–505. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58469-0_33

European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (2019). https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en. Accessed 19 Apr 2021

European Parliament: 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)

Hammer, M.: What is business process management? In: Handbook on Business Process Management, vol. 1, pp. 3–16. Springer, Berlin (2015)

Henriksen-Bulmer, J., Faily, S., Jeary, S.: DPIA in context: applying dpia to assess privacy risks of cyber physical systems. Fut. Internet **12**(5), 93 (2020)

-FTI 2020: Annual governance report. Technical report (2021) https://iapp.org/media/pdf/resource_center/IAPP_FTIConsulting_2020PrivacyGovernanceReport.pdf. Accessed 19 Apr 2021

ISO 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements (2013)

Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: the PriS method. Requirem. Eng. **13**(3), 241–255 (2008)

Kalloniatis, C., Kavakli, E., Gritzalis, S.: Methods for designing privacy aware information systems: a review. In: 2009 13th Panhellenic Conference on Informatics, pp. 185–194. IEEE (2009)

Kokolakis, S.A., Demopoulos, A.J., Kiountouzis, E.A.: The use of business process modelling in information systems security analysis and design. Inf. Manag. Comput. Secur. **8**(3), 107–116 (2000)

Langheinrich, M.: Privacy by design — principles of privacy-aware ubiquitous systems. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) Ubicomp 2001: Ubiquitous Computing. UbiComp 2001. LNCS, vol. 2201, pp. 273-291. Springer, Berlin (2001). https://doi.org/10.1007/3-540-45427-6_23

McKinsey &Company: GDPR compliance since May 2018: A continuing challenge (2019). https://www.mckinsey.com/business-functions/risk/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge. Accessed 19 Apr 2021

Mellado, D., Blanco, C., Sánchez, L.E., Fernández-Medina, E.: A systematic review of security requirements engineering. Comput. Stand. Interf. **32**(4), 153–165 (2010)

Pullonen, P., Matulevičius, R., Bogdanov, D.: PE-BPMN: privacy-enhanced business process model and notation. In: International Conference on Business Process Management, pp. 40–56 (2017)

Spiekermann, S., Acquisti, A., Böhme, R., Hui, K.-L.: The challenges of personal data markets and privacy. Electron. Mark. **25**(2), 161–167 (2015). https://doi.org/10.1007/s12525-015-0191-0

Reuters, T.: Study finds organizations are not ready for GDPR compliance issues (2019). https://legal.thomsonreuters.com/en/insights/articles/study-finds-organizations-not-ready-gdpr-compliance-issues. Accessed 19 Apr 2021

Tom, J.: Assessing and improving compliance to privacy regulations in business processes. In: Proceedings of the Doctoral Consortium papers presented at 30th International Conference on Advanced Information Systems Engineering (CAiSE) (2018)