7-4-2022

A Review of GDPR Impacts on Information Security

Pauliina Hirvonen
University of Jyväskylä, pauliina.a.hirvonen@student.jyu.fi

PACIS 2022 A Review of GDPR Impacts on Information Security

Completed Research Paper

Pauliina Hirvonen
University of Jyväskylä, Finland
pauliina.a.hirvonen@student.jyu.fi

Abstract

The aim of this literature review is to understand GDPR impacts on information security in organisations. The research question is: What outcomes previous research reveal about the GDPR impacts on information security development? Findings indicated that GDPR has had several impacts divided in six categories here: user profiling and data collection, business impacts, management and compliance, personal competences, skills and career, authorisation, authentication and notification obligation and data storage. Findings also indicated that even though GDPR had upraised information security and data protection requirements, it has caused also challenges. Previous research raised important separate issues of GDPR impacts of information security, but did not addressed topic comprehensively. Previous literature did not report best practices of how organisational GDPR impacts are examined. To fill this gap, the framework for observing GDPR impacts of organisations was built.

Keywords: General Data Protection Regulation, Privacy and Data protection development, GDPR and Information systems research, GDPR impacts, Organisational perspective of GDPR, Information security improvement, International legislation of information security

Introduction

It was declared by the European Union (EU) officials in 2018, that the General Data Protection Regulation (GDPR) as being a single rule package would be simpler and cheaper for the organisations doing business in the EU. However, based on the previous literature, the first impressions of GDPR generally also included fear of implementation and interpretation challenges. The organisations widely around the world processing EU residents' personal data have been the key actors turning a theory into practice. The aim of this literature review is to understand GDPR impacts on organisational information security through the existing research. The research question is: What outcomes previous research reveal about the GDPR impacts on information security development? The novel and widely involving nature of the regulation makes the issue exciting to research.

Findings indicated that GDPR has had several impacts and these impacts reported in previous research were divided in six categories: *user profiling and data collection, business impacts, management and compliance, personal competences, skills and career, authorisation, authentication and notification obligation and data storage*. Findings also indicated that even GDPR had upraised information security and data protection requirements, it has not managed to guide the implementation as well as expected and also other challenges imposed. Previous research raised important separate issues of GDPR impacts of information security, like third party cookies (e.g. Hu & Sastry, 2019), password management strengthening (Raponi & Pietro, 2020) or GDPR skills requirement (Florea & Stray, 2019), but no wider conclusions of GDPR impacts based on results can be made. Previous literature did not report best practices or any framework of how organisational GDPR impacts are examined. These research gaps, as well as findings

were used to formulate the framework for observing GDPR impacts of organisations. Therefore, the proposed research framework for future research is considered as the main contribution of this work to support the future research of this topic.

The research has the following structure: at first, the short background and the definitions of keywords are introduced. Then, the methodological choices and the realisation of the research are presented. The results and findings of the analysis follow that. Finally, the discussion and conclusions are located at the end of the paper.

A Brief Introduction to the Research Field

In this section, a strict bind between the GDPR and information security are defined and the expected results are shortly discussed.

The Relationship of the GDPR and Information Security

GDPR (Regulation (EU) 2016/679) is the European Union´s regulation for the protection, processing and free movement of EU residents´ personal information. According to official EU pages, the aim of it is to strengthen individuals' fundamental rights, facilitate business by clarifying rules for companies and public bodies to facilitate business in the digital single markets and decrease the fragmentation in different national systems and unnecessary administrative activities. (EU, 2022). According to the European Data Protection Supervisor (EDPS), the EU's data protection laws are valued globally as a "gold standard" (2020). The regulation is also seen e.g. as a concept of privacy as a fundamental human right (Goddard, 2017), or a major step for harmonising data protection rules and privacy and security promotor (Baxevani, 2019). GDPR is also referred to global new challenges and potential opportunities caused by enormous data protection activities (Li, Yu & He, 2019). Conroy et al. (2014) defined GDPR as a potential competitive advantage, if consumer trust can be achieved.

GDPR and information security relationship can be approached in several ways. One approach for GDPR and information security relationship is to see GDPR as an envoy of privacy and data protection, which is strongly connected to information and cyber security wholeness development. Consumers' personal information are for example seen as a threat by information security breaches and hardware vulnerabilities leading to financial crimes and identity thefts (Hawk, 2018). On the other hand, Capgemini reported in 2018 that strengthening consumers' trust with privacy and security led to more sales increasing the competitive advantage of organisations. Basic requirements of GDPR for privacy and data protection are presented in its article 5, and the requirements (e.g. data anonymizing, data breach notifications or safety data transfer across borders) set data protection and privacy naturally under wider meaning of organisational information security, since those expect carefully planned information secure measures (Li, Yu & He, 2019). Information security is a necessary tool for practical data protection implementation. Whitman and Mattord (2011) emphasised the importance of information security management (ISM) and data and network security related to security controls demanded by GDPR.

Expected Results

The regulation defines the following data protection principles: transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability (European Data Protection Board, 2020). However, the practical guidance for how to implement it is missing. Examples (GDPR.eu, 2022) of the accuracy with which some GDPR principles of all seven (Article 5.1-2) are guided are presented in table 1. The expected results relate, among others, to supplementing this guidance.

Accountability	*Data controllers have to be able to show their GDPR compliance in practice.*
Consent	*Data consent must be "freely given, specific, informed and unambiguous"* *Requests for consent must be clearly distinguishable from the other matters and presented in clear language.* *Data subjects can withdraw previously given consent whenever they want, and their decisions have to be honoured. The legal basis of the processing to one of the other justifications can not be changed.* *Children under 13 can only give consent with permission from their parents.* *Documentary evidence of consent has to be kept.*
Data security	*Data has to be handled securely by implementing appropriate technical and organisational measures.*
Data protection by design and by default	*Already in the planning phase the data protection principles in the design of any product or activity have to be considered .*
Purpose limitation	*Processing data for legitimate purposes specified explicitly to the data subject.*

Table 1. Examples of the guidance of some GDPR requirements in accordance with GDPR.eu (2022).

Methodology and the Research Process

In this section a research methodology and research process are presented.

Literature Review

A highly standardised literature review in IS field is clearly restricted and the phases of the process, such as data collection and analysis, are precisely described (Webster and Watson, 2002; Rowe, 2014; Schryen, 2015; vom Brocke et al, 2015; Paré et al., 2016; etc.). Based on the background of the research field it was noticed that information gaps of the existing literature needed to be found to justify the grounds for the further empirical research. According to Webster and Watson (2002), a literature review can be used to pinpoint the areas for further examination.

A descriptive literature review used in this work does not necessarily include strict protocols or rules of material collection, but still allows for adding boundaries, if it is favourable for the research. A descriptive review was approached as the most adequate method for this research issue, because it focuses on enhancing interpretable themes from the research material (Guzzo et al, 1987). It suits well in purpose, because the aim of the research was to observe existing themes found in existing literature in the IS field. Theming and categorisation, which King and He (2005) noted to be important related to identifying trends and patterns, allows a consistent and linked approach to research material throughout the process. Through the themes, the comparison and processing of the sub-groups through different kinds of frequency analysis forms becomes more complete. Referring to other styles, for example a narrative review is far more vulnerable for subjectivity, because of lacking generally approved procedures (Guzzo et al., 1987). Systematic literature, on the other hand, is not a suitable method for rather fresh issues like GDPR impacts, where it is expected to have quite a limited amount of existing literature, descriptive review then enables the usage of wider research material (Evans 2008: 137).

Quality aspects are an important part of scientific research and the processes and criteria of research evaluation may depend on the nature and objectives of the research (Biagetti, Gedutis & Ma, 2020). Snyder (2019) criticised the quality and reliability of the traditional reviews, like descriptive, of lacking comprehensiveness and adherence to a particular method. He remained (Snyder, 2019), that the analysis method should support answering the research question. The aim of the work is to draw a view of existing

themes and approaches for GDPR impacts. Typical analysing methods used with descriptive review can be for example theming and categorising. The quality of the research consists of validity and reliability (Edmonds & Kennedy, 2012). Validity means if the research actually measures what it is intended to measure (The University of Alberta, 2022). Here it also means selecting qualified data collection sources and collecting information accurately and taking into account also the unfamiliar information to be assessed (Alleydog.com's online glossary, 2022). Documentation of the process and its finding will support the reliability of the research. According to dissertation adviser John Dudovskiy (2022), reliability is the degree to which a research method contributes stable and consistent results, but it also refers to the consistency and stability of measures and results (The University of Alberta, 2022). Also, transparency during the life cycle of this research process was an approach to increase the validity, reliability and trustworthiness. Every phase and step of the work is carefully documented and reasoned.

According to Elo and Kyngäs (2008), transparency is an effective manner to meet ethical challenges. Biagetti, Gedutis and Ma (2020) have divided research evaluation ethics in two: 1) Research ethics, including; rigour, reliability, respect, responsibility, honesty, etc., and 2) Evaluation ethics, including: respect for autonomy, nonmaleficence, beneficence, responsibility, justice, fidelity, competence, integrity, free of bias etc. These aspects have been taken into account in the design of the study.

Research Process Implementation

Research process was implemented paraphrasing by Cooper´s model (1989: 15) including five steps: 1. Problem Setting, 2. Data Acquisition, 3. Evaluation, 4. Analysis and Interpretation, and 5. Presentation. In this section, problem setting, data acquisition and evaluation are discussed. Analysis and presentation are implemented in Analysis and Discussion sections.

Problem Setting

Problem setting included research aim, defining research question, data sources, search strings and inclusion criteria. The aim was to understand GDPR impacts on information security in organisations through the existing academic research. The research question was: What outcomes previous research reveal about the GDPR impacts on information security development? Data sources were defined (see "Data Acquisition"). Search strings were: a) GDPR OR "general data protection regulation" AND "impact" OR "effect", b) GDPR OR "general data protection regulation" AND "information security" OR "information systems", c) GDPR OR "general data protection regulation" AND "impact" OR "effect" AND "information security. Inclusion criteria contained the following: written in English, scientific papers of academic publishing channels, published between 2016 – 2020.

Data Acquisition

Data acquisition refers to data collection and filtering. Research material was collected from Computers & Security, Information and Computer Security, The Journal of Information System Security, Information Security Journal (A Global Perspective), Association for Computing Machinery Digital Library (ACM) and Institute of Electrical and Electronics Engineers and Institution of Engineering and Technology (IEEE) Xplore Digital Library. These sources are generally scientifically appreciated. Data search was done between 8 – 11/2020 and as a result, totally 627 peer reviewed articles in the IS field published between the years 2016 – 2020 were found. The majority of them were from ACM.

Evaluation

Evaluation included four phases: 1) Evaluation, 2) First screening, 3) Second screening and 4) Analysis of the core material. After the data search, all the 627 articles were evaluated and articles that did not pass inclusion criteria (see Problem Setting) were rejected. 457 articles were left after the evaluation and were once again read through, and here the articles that were not concerned with GDPR were eliminated. At the end of the first screening, 133 articles remained. The second screening included categorising and dividing 133 articles in four themes: A GDPR impacts, B Solutions (different kinds of innovation), C Privacy history and D Comparison of privacy legislation. This research focused next on examining closer the actual theme, namely A GDPR impacts which contains 31 articles as a core research material. Generally, the finding of

adequate articles required several readings and theming content two times. Theming supported sorting these closest relevant 31 articles from others. About 26 % (31) of all evaluated IS GDPR related studies were connected to the original research issue. The analysis of the core research material (31 articles) is discussed in the next section.

Results and Analysis of the Findings

Results and analysis of findings are presented in this section. Theming and classifications was used as an analysing method through the process to clarify the interferences of the research approaches. Classical thematic analysis was used to lift the relevant content of the studies examined.

In general, there is a lot of research related to GDPR, especially from the technological and legislation fields. This finding is also supported by Lisiak-Felicka and Szmit (2021). There arose several different kinds of challenges related to regulation, not least a lack of clarity of the regulation but also surrounding the interaction between EU law and public international laws. More precise GDPR guidance was called for that organisations, so that especially SMEs could ensure their capacity to fulfil requirements and on the other hand maintain privileges and immunities (Kuner, 2020). The importance of information security for GDPR compliance was emphasised many times. The amount of the research trying to interpret the regulation proved that the regulation is not only topical, but also theoretically and practically commonly felt as an opaque and difficult issue. Generally, research frames elaborated e.g. GDPR related problem recognition; theoretical or practical implementation of the regulation or practical problem solving; concerning typically some technical solutions and innovations. Typical general IS field GDPR research also aimed to predict the further impacts of the implementation. These findings are in line with other studies. Existing GDPR research has e.g. found to address recommendations or assess compliance, identify success factors, technical issues (Tatara, Gokceb & Nussbaum, 2020) or other challenges (e.g. Alizadeh et al., 2019).

The findings indicated that by the year 2020 there would be a limited amount of academic articles on GDPR impacts on information security, even though there was a lot of research of GDPR impacts in general. The majority of previous research in the information security field were empirical studies that focused on solving GDPR requirements of concrete life rather than addressing scientific procedures.

Research material was analysed from several perspectives (sources, year of publication, time of examination, research methods, academic quality, content, findings, contributions, gaps etc.). 31 articles were found from four sources: ACM (81 %), ICS 3(%), IEEE (3 %) and CS (3 %). None of the chosen articles were published in 2016, obviously because the issue was so topical and only one was published in 2017. The growth of publishing has been moderately flat after 2018 (7), 2019 (11) and 2020 (12). Material found from ACM, total 25 articles, dominated every year. The first accepted articles from Information & Security and Information and Computer Security journals were published only in 2020. All in all, analyses based on either publication year or source did not provide specific useful observations.

The time of examination varied and 12 of 31 articles did not mention at all when the research was conducted. For 13 articles, the research was run lasting for a maximum of one year. For those articles that contained information on the time of the research (19), the majority (9) at the time of the study were 2018. The longest examination lasted 9 years (Nabbosa & Iftikhar, 2019), already starting in 2010 and was integrated into the GDPR when that entered into force. Of all the articles that reported their time (18), five lasted more than one year: two articles lasted for two years, one article for three years, four years and nine years. The most recent research was examined in 2020.

Research methods varied: 5 articles (16,1 %) did not report any information on research methods at all, 17 empirical (54,8 %), 6 theoretical (19,3 %) and 3 mixed-methods (empirical-theoretical) (9, 7 %) as minority. The distribution of the articles cannot be entirely certain, as the methods were not clearly presented in all studies and were based on the researcher's conjecture and evaluation. There were some positive exceptions of material, like Hargitai, Shklovski and Wasowski (2018) with their thorough grounded theory research. Some had explained the method in detail and also evaluated its usefulness (Sağlam & Nurse, 2019; Utz et al., 2019; Jakobi et al., 2020 etc.). Unfortunately, about a half of the articles focused on empirical implementation (Almada, 2019; Hus & Sastry, 2019; Monteiro-Krebs et al. 2019; Sánchez-Monedero,

Dencik & Edwards, 2020 etc.), forgetting to document measures and phases. On the other hand, the implementation process of the empirical research might have been explained in detail, but the research method might not have been named and the analysis method was missing (For example Sanchez-Rola et al., 2018 etc.). The largest individual empirical groups were interviews and unnamed empirical studies. The majority, totally 29 of the 31 articles did not contain a quality assessment. Six theoretical studies included 1 Ethics Canvas and 1 Quantitative and qualitative research, and 4 no-name theoretical studies (except that one referred to the model of Webster and Watson, 2002). There also were three mixed empirical-theoretical studies: 1 Literature review + interview, 1 Literature review + survey and 1 No-name mixed. N/O means that the current aspect is not mentioned in the research. In some cases, the implementation of the research was described in detail, but no name was found for the method. The studies also did not assess the suitability of the method and its impact on the results. Another major shortcoming is the poor academic quality of research, which also means that the results of previous research can hardly be generalised. Unfortunately, the lack of appropriate academic procedures may hinder the contribution of existing literature.

What it comes to content, previous research highlighted important but separate aspects and interesting anecdotes of GDPR impacts on information security. GDPR general nature seems to be regarded as hazy and nebulous, so especially challenges in different areas of GDPR implementation were awaited to be reported. It was noticed that GDPR implementation will require remarkable efforts and resources in organisations. Dellinger wrote in 2019 that basing on empirical findings, more than half of all websites under the GDPR failed to present privacy policies for consumers with adequate manners. Several studies revealed this ambiguity in GDPR requirements and a lack of practical guidance for end-users and companies. Some researchers (e.g. Tankard, 2016; Sirur, Nurse & Webb, 2018) emphasised the challenges for organisations of interpreting GDPR and its requirements, since GDPR did not provide clear guidelines for adequate technological solutions and implementation. De Arriba-Sellier (2018) also reported on the lack of clarity of GDPR. Indeed, much of the research material here involved various attempts to interpret or produce solutions or tools to meet the requirements (for example Geko & Tjoa, 2018; Sobers, 2018). Studies revealed also that the level of GDPR knowledge and understanding of the organisations studied varied significantly (for example Alizadeh et al., 2019; Breitbarth, 2019). Some articles presented the importance of the research phenomenon (e.g. Hoel, Griffiths & Chen, 2017) or raised an awareness of some certain important issues related to GDPR (e.g. Biega et al., 2020). Almost without exception, articles highlighted the huge importance of information security as part of the GDPR.

Technological, information and cybersecurity development, for example everyday platforms used for news personalisation and related forms of information (Monteiro-Krebs et al., 2019), were mentioned relating essentially to GDPR compliance. Li, Yu and He (2019), among others, pointed out the importance of IS and IT in solving important compliance challenges, e.g. emerging technologies (artificial intelligence (AI), blockchains (BC) and cloud computing (CP)) as decreasing the performance and productivity aspects of organisations. Mackay (2017) detailed especially needs for personal data identification measures and holistic search tools to detect and extract data in organisations, and detected the GDPR influences for technology platforms and data architecture. In the case of blockchains, Wallace and Castro (2018) concerned the challenge of identifying the controller and difficulty for each node to perform strict requirements. GDPR consequences for organisations' cybersecurity policy and practices were also predicted (Li, Yu & He, 2019). Withey (2018) raised cybersecurity training and education measures as important both for governments and private organisations.

Among technological aspects, Freitas and da Silva (2018) pointed to expectations of required GDPR efforts including also legal and functional change, that would, over the sector and industry restrictions, cause major impacts for organisations. Boban (2018) assessed that impacts would include wider reconsideration of overall data processing practices, new measures, policies and re-design of processes. In terms of the nature of the organisations, GDPR was estimated (Seo et al., 2017) to cause challenges especially for so called information sensitive organisations (processing large amounts of personal data). On the other hand, relating to company size and branch, it was concluded that larger technology firms could resource more on GDPR compliance than smaller institutions (Jo & Gebru, 2020). Jia and Wagnan (2020) highlighted organisational impacts from value propositions perspective through product design, personalised services, customer engagement and monetisation. Houser and Voss (2018) assessed GDPR impacts on business models (e.g. in advertising) from the privacy perspective.

Finally, GDPR impacts for information security reported by previous research (31 articles) were divided here totally in six categories by their contents: 1) User profiling, 2) Business impacts, 3) Management and compliance, 4) Personal competences, skills and career, 5) Authorisation and notification obligation and 6) Data storage. When concerning the results of the GDPR impacts, User profiling and data collection had been the most constant main research theme in years 2017 – 2019 and included more than half of all research (figure 1). Business impacts, management and compliance, personal competences, skills and career, and authorisation and notification obligation evenly distributed into the next largest group. Research of data storage presented as a minority. The sub-groups of these six impact categories are presented in figure 1. User profiling and data collection had the most sub-groups (17). Business impacts, authorisation, authentication and notification obligation, management & compliance, personnel competence, skills & career were the second largest sub-groups (3 in each). Data storage was the smallest one with two sub-groups.

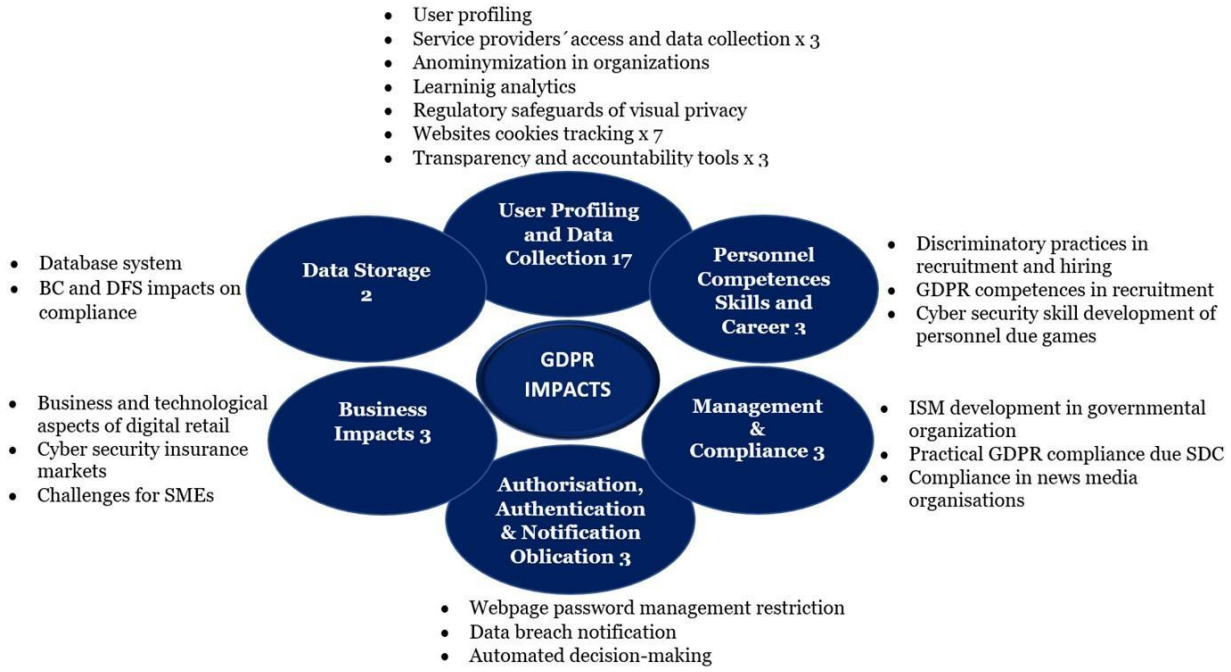

Figure 1. Themes with sub-groups.

Some articles noted clearly that GDPR has had a very wide range of effects (for example Teixera et al., 2019), but none of the articles aimed to cover all these effects and did not explain through what kind of process or framework GDPR impacts in organisations is suggested to observe or assess. Previous research on GDPR impacts for information security did not manage to raise the level of scientific research in the IS field. Overall, the studies left a fragmented and incomplete picture of the GDPR impacts. The incompleteness and gaps of previous research justify the need for further research.

Discussion

Descriptive literature review provided a landscape of the status and shortcomings of existing research due to screening, theming and classifying. If the research data is observed as a whole, it can be seen that the comparability of the works is challenging because of several differences; like varying research aspects and aims, approaches, methods, location, organisation, industry and frameworks. However, it is interesting that the themes of different categories were quite easy to identify. Through the thematic analyses, previous research of GDPR impacts for information security was divided in six categories: user profiling and data collection, business impacts, management and compliance, personal competences, skills and career, authorisation and notification obligation and data storage. Previous research raised several interesting details of impacts discussed in the previous section, but it also focused strongly towards technical issues

leaving out several areas of information security. This does not automatically mean that areas other than examined are not impacted by GDPR, but at least they are less examined, perhaps because it is easier to focus on research on one single aspect of GDPR impacts. However, it is not possible to assess the overall GDPR impacts for information security in organisations unless all areas of information security are not considered. This research is important because it offers a practical and clear understanding of the research gaps of previous literature to further examination to fulfil.

A research framework consisting of six research (figure 2) aspects are built basing the findings raised through review. This research framework is proposed due to the absence of the academic practices for observing GDPR impacts comprehensively.

Figure 2. A chronological research framework for the future.

The following conclusions were especially considered when building the framework: 1) The initial expectations of GDPR requirements were unclear for organisations due inadequate official guidance (For example Tankard, 2016; Sirur et al, 2018;). 2) The organisational practices of building and the levels of situational awareness of GDPR requirements varied significantly (for example Alizadeh et al., 2019; Breitbarth, 2019). 3) There are no clear and uniform practices for evaluating information security development (Withey, 2018). 4) The future GDPR expectations relate to progress of official guidance (For example De Arriba-Sellier, 2018). 5) GDPR has improved information security in multiple ways (Teixera et al., 2019). Also aspects other than technical should be observed (For example Boban, 2018; Freitas & da Silva, 2018) comprehensively. Based on the conclusion of this review, the overall improvements are uncovered by the academic research. 6) And finally, since the GDPR is still an ongoing process, the impacts should be observed as an ongoing logical and chronological process.

This research can provide interesting insights especially for official GDPR authorities and law developers. It is hoped to encourage researchers to test and create new approaches to observe complex research issues like this. Research findings are also wished to note the organisational GDPR managers and data protection organisations to concern GDPR impacts comprehensively and taking into account the individual organisational aspects. Assessing GDPR impacts is also an area, which could be supported by partners and service providers of the organisations.

Speaking of limitations, it cannot be said that the true taxonomy of GDPR impacts could have been found through previous research with weak academic contributions. Another limitation was the validity because of the short time period, totally four years. Basing the research in a wider time period could have increased validity and generated more accurate results. Because GDPR keeps on developing all the time, it is reasoned

to be regularly assessed. The logical next step in the future would include testing of the proposed chronological research framework. Future empirical research would also increase the awareness of GDPR and therefore cause more effective impacts for it. From the user perspective, Anderson and con Seck (2020) had concluded likewise, that creating understanding of GDPR would also enhance users´ security senses, so it can be estimated the possible influence for other areas also.

Conclusions

The aim of this literature review was to understand GDPR impacts on information security in organisations. The research question was: What outcomes previous research reveal about the GDPR impacts on information security development? Findings indicated that GDPR has had several impacts that even GDPR had upraised information security and data protection requirements, it has not managed to guide the implementation as well as expected and also raised following issues: 1) GDPR has improved organisational information security, but the overall improvements were uncharted; 2) a lack of shared practices regarding data protection (DP) and information security development evaluation and GDPR impact observation; 3) GDPR found to have several impacts on different layers in organisations, but these had not accumulated in previous literature. Six categories of GDPR impacts (with sub-groups) were recognised and it was noticed that previous research faced the issue mainly from a single technical side. Previous research did not comprehensively approach GDPR impacts on information security, nor explain how GDPR impacts are suggested to observe. Lean and clear practices to assess and report GDPR impacts are still unknown for academic research. This research is important because it highlighted the impacts of GDPR noted by previous research but also suggested a chronological framework for future research to observe organisational GDPR impacts. The results of this work is hoped to benefit researchers and decision makers.

References

Alizadeh, F., Jakobi, T., Boldt, J. and Stevens, G., 2019. "GDPR-Reality Check on the Right to Access Data: Claiming and Investigating Personally Identifiable Data from Companies" in *Proceedings of Mensch und Computer 2019* (MuC'19), pp. 811-814.

Alleydog.com´s online glossary. 2022. Official webpages. "Descriptive Validity". (n.d.) in *Alleydog.com's online glossary*. https://www.alleydog.com/glossary/definition-cit.php?term=Descriptive+Validity

Almada, M. 2019. "Human intervention in automated decision-making: Toward the construction of contestable systems", in *ICAIL* June 17–21, 2019, pp. 2-11. Montreal, QC, Canada https://doi.org/10.1145/3322640.3326699.

Anderson, D., and von Seck, R. 2020. "The GDPR and its impact on the we", in *Network Architectures and Services*. Seminar IITM SS 20. 11/2020. https://doi.org/10.2313/NET-2020-11-1_01. https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2020-11-1/NET-2020-11-1_01.pdf.

Asghar, M., Kanwal, N., Lee, B., Fleury, M., Herbst, M. and Qiao, Y. 2019. "Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective", in *IEEE Access*. 7. 111709-111726. 10.1109/ACCESS.2019.2934226.

Bahsi, H., Franke, U. and Friberg, E. 2019. "The cyber-insurance market in Norway", in *Information & Computer Security*. ahead-of-print. 10.1108/ICS-01-2019-0012.

Bargh, M.S, Meijer, R., Vink, M., van den Braak, S., Schirm, W. and Choenni, S. 2019. "Opening Privacy Sensitive Microdata Sets in Light of GDPR: The Case of Opening Criminal Justice Domain Microdata", in *Proceedings of dg.o 2019: 20th Annual International Conference on Digital Government Research* (dg.o 2019), June 18, 2019, Dubai, United Arab Emirates. ACM, New York, NY, USA,.https://doi.org/10.1145/3325112.3325222.

Baxevani, T. 2020. *GDPR Overview. Project: Privacy and Data Protection in European Union*. Retrieved 05.05.2020 from https://www.researchgate.net/publication/333560686_GDPR_Overview.

Biagetti, M. T., Gedutis, A. and Ma, L. 2020. "Ethical Theories in Research Evaluation: An Exploratory Approach", in *Scholarly Assessment Reports*, (2:1), pp. 11. http://doi.org/10.29024/sar.19.

Biega, A.J., Potash, P., Daumé III, H., Diaz, F. and Finck, M. 2020. "Operationalizing the Legal Principle of Data Minimizationfor Personalization", in *Proceedings of the 43rd International ACM SIGIR*. Conference on Research and Development in Information Retrieval (SIGIR '20), July 25–30, 2020, Virtual Event, China. ACM, New York, NY, USA. https://doi.org/10.1145/3397271.3401034.

Boban, M. 2018. "Protection of Personal Data and Public and Private Sector Provisions in the Implementation of the General EU Directive on Personal Data (GDPR)", in *27th International Scientific Conference on Economic and Social Development,* Rome, pp. 161-169.

Breitbarth, P., 2019. "The impact of GDPR one year on", in *Network Security*, (2019:7), Pp. 11-13. European Commission, 2019. General Data Protection Reglation shows results but work needs to continue. Press Release. Available online: https://gdpr-info.eu.

Casino, F., Politou, E., Alepis, E. and Patsakis, C. 2019. "Immutability and Decentralised Storage: An Analysis of Emerging Threats", in *IEEE Access*. pp. 1-1. 10.1109/ACCESS.2019.2962017.

Chivot. E. and Castro, D. 2019. *What the evidence shows about the impact of the gdpr after one year*. Retrieved 12.1.2022 from https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/.

Cooper, H. 1998. *Synthesizing Research: a Guide for Literature Reviews*. Thousand Oaks: Sage Publications, Inc.

Conroy, P., Narula, A., Milano, F., and Singhal, R. 2014. *Building consumer trust - Protecting personal data in the consumer product industry*. Retrieved December 21, 2018, from https://www2.deloitte.com/insights/us/en/topics/risk-management/consumer-data-privacy-strategies.html.

de Arriba-Sellier, N. 2018. "GDPR: the risks of empowering lawyers, not citizens", in *Leiden law blog*. Retrieved 11.2.2022 from https://leidenlawblog.nl/articles/gdpr-the-risks-of-empowering-lawyers-not-citizens.

Dellinger, A.J. 2019. "A Year Later, Many Sites Are Still Failing to Meet Basic GDPR Requirements", in *FORBES* Blog text, 31.5. 2019. Retrieved 12.1.2022 from https://www.forbes.com/sites/ajdellinger/2019/05/31/a-year-later-many-sites-are-still-failing-to-meet-basic-gdpr-requirements/?sh=5025963d1eb9.

Dudovskiy. J. 2022. Official websites. Business Research-Methodology. Retrieved 28.2.2022 from https://research-methodology.net/research-methodology/reliability-validity-and-repeatability/research-reliability/.

Edmonds, W. A., and Kennedy, T. D. 2012. *An applied reference guide to research designs: Quantitative, qualitative, and mixed methods.* Thousand Oaks, CA: Sage.

Elo, S. and Kyngäs, H. 2008. "The qualitative content analysis process", in *Journal of Advanced Nursing* (62:1), pp.107–115.

European Data Protection Board. (2020). Guidelines 4/2019 on Article 25. Data Protection by design and by Default. Version 2.0. Adopted on 20 October 2020. Principles outlined in Retrieved 19.3.2022 fromo https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

European Data Protection Supervisor European Union. (2020). Official Web pages." 4.5.2020: EDPS The History of the General Data Protection Regulation". Retrieved 04.05.2020 from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en EU and International organizations: GDPR and International Organizations January 2020. https://doi.org/10.1017/aju.2019.78 LicenseCC BY 4.0.

European Union. 2018. The GDPR: new opportunities, new obligations. What every business needs to know about the EU's General Data Protection Regulation. https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf

European Union official website 2022. Data protection. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en.

Evans, D. 2008. "Overview of Methods", in *Reviewing Research Evidence for Nursing Practice: Systematic Reviews*, pp. 137–148. Edit. Christine Webb & Brenda Ross. Oxford: Blackwell Publishing.

Fazzini, K. 2019. *Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators*. Retrieved from https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-andregulators.html.

Field, E.L. 2020. *United States Data Privacy Law: The Domino Effect After the GDPR*. 24 N.C. BANKING INST. 481. https://scholarship.law.unc.edu/ncbi/vol24/iss1/21 See also: http://www.ncsl.org/research/telecommunications-and-information-technology/datasecurity-laws.aspx.

Florea, R. and Stray, V. 2019. "A Global View on the Hard Skills and Testing Tools in Software Testing", in *ACM/IEEE 14th International Conference on Global Software Engineering* (ICGSE), 2019, pp. 143-151, https://doi.org/10.1109/ICGSE.2019.00035.

Freitas, M.C. and da Silva, M. 2018. "GDPR Compliance in SMEs: There is much to be done", in *Journal of Information Systems Engineering & Management*, (34:4), pp. 30.

Geko. M. and Tjoa, S. 2018. "An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security", in *Proceedings of the Central European Cybersecurity Conference 2018* (CECC 2018). Association for Computing Machinery, New York, NY, USA, Article 19, pp. 1–6. https://doi.org/10.1145/3277570.3277590.

Goddard, M. 2017. "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact", in *International Journal of Market Research*, (59:6), pp. 703–705. https://doi.org/10.2501/IJMR-2017-050.

GDPR.EU. 2022. Ben Wolford blog text. "What is GDPR, the EU's new data protection law?" Retrieved 18.03.2022 from https://gdpr.eu/what-is-gdpr.

Guzzo, R.A., Jackson, S.E., and Katzell, R.A. 1987. "Meta-Analysis Analysis", *in Research in Organizational Behavior* (9), pp. 407-442.

Habib, H., Pearman, S., Wang, J., Zou, Y., Acquisti, A., Cranor, L.F., Sadeh, N. and Schaub, F. 2020 . ""It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices", in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376511.

Hargitai, V. Shklovski, I. and Wasowski, A. 2018. "Going Beyond Obscurity: Organizational Approaches to Data Anonymization", in *Proceedings of the ACM on Human-Computer Interaction*, (2), pp. 1-22. https://doi.org/10.1145/3274335.

Hawk, L. 2018. A Blog writing. *Data Privacy Day 2018: Data Breaches, Harm, and Culture, Privacy Watch*. 29.1.2018. Bloomberg law. Law reports.

Hoel, T., Griffiths, D. and Chen, W. 2017."The influence of data protection and privacy frameworks on the design of learning analytics systems", in *The Seventh International Learning Analytics & Knowledge Conference*, LAK '17, March 13 - 17, 2017, Vancouver, BC, Canada. pp. 243-252. https://doi.org/10.1145/3027385.3027414.

Houser, K and Voss, W. 2018. "Gdpr: The end of google and facebook or a new paradigm in data privacy?", in *SSRN Electronic Journal*.

Hu, X. and Sastry, N. 2019. *Characterising Third Party Cookie Usage in the EU after GDPR*. https://doi.org/10.1145/3292522.3326039.

Ireland´s Data Protection Commissioner. 2005. *16th Annual Report 2004*. Tuarascáil Bhliantúil. Data Protection Commissioner of Ireland. 15.3.2005. Retrieved 22.1.2022 from https://www.dataprotection.ie/sites/default/files/uploads/2018-12/annual_report_2004.pdf.

Jakobi, T., Stevens, G., Seufert, A., Becker, M. and von Grafenstein, M. 2020. *Web Tracking Under the New Data Protection Law: Design Potentials at the Intersection of Jurisprudence and HCI*. i-com, (19), pp. 31-45. https://doi.org/10.1515/icom-2020-0004.

Jia, J. and Wagnan, L. 2020. "The One-Year Impact of the General Data Protection Regulation (GDPR) on European Ventures", in *Data catalyst*. https://datacatalyst.org/wp-content/uploads/2020/01/GDPR-report-2020.pdf.

Jo, E.S. and Gebru, T. 2020. *Lessons from Archives: Strategies for Collecting Sociocultural Data in Machine Learning*. https://doi.org/10.48550/arXiv.1912.10389.

Khalil, M., Prinsloo, P. and Slade, S. 2018. "The unbearable lightness of consent: mapping MOOC providers' response to consent", in *The Fifth Annual ACM Conference Learning at ScaleAt*, pp. 1-11. London, United Kingdom. https://doi.org/10.1145/3231644.3231659.

Karegar, F., Pettersson, J.,S. and Fischer-Hübner, S. 2020. "The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention", in *ACM Transactions on Privacy and Security*, (23), pp. 1-38. https://doi.org/10.1145/3372296.

King, W.R. and He, J. 2005. "Understanding the Role and Methods of Meta-Analysis in Is Research", in *Communications of the Association for Information Systems* (16), pp. 1.

Kirchner, E. A., Fairclough, S. H., and Kirchner, F. 2019. "Embedded multimodal interfaces in robotics: applications, future trends, and societal implications", in *The Handbook of Multimodal-Multisensor Interfaces: Language Processing, Software, Commercialization, and Emerging Directions*. Association for Computing Machinery and Morgan & Claypool, pp. 523–576. https://doi.org/10.1145/3233795.3233810.

Kröger, J.L., Lindemann, J. and Herrmann, D. 2020. "How do App Vendors Respond to Subject Access Requests? A Longitudinal Privacy Study on iOS and Android Apps", in *The 15th International*

Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland. ACM, New York, NY, USA, https://doi.org/10.1145/ 3407023.340705 .

Kuner, C. 2020. "The GDPR and International Organizations", in *AJIL Unbound*, (114), pp. 15-19. https://doi.org/10.1017/aju.2019.78.

Kulyk, O., Hilt, H., Gerber, N. and Volkamer, M. 2020. *This website uses cookies: Users' perceptions and reactions to the cookie disclaimer*. Retrieved 12.1.2022 from https://www.researchgate.net/publication/325923893_This_Website_Uses_Cookies_Users'_Perceptions_and_Reactions_ to_the_Cookie_Disclaimer, 2018, online; accessed 02 May 2020.

Li, H., Yu, L. and He, W. 2019. "The Impact of GDPR on Global Technology Development", in *Journal of Global Information Technology Management*, (22), pp. 1-6. https://doi.org/10.1080/1097198X.2019.1569186.

Lisiak-Felicka, D., and Szmit, M. 2021. "GDPR implementation in public administration in Poland – 1.5 year after: An empirical analysis", in *Journal of Economics & Management*, (43), pp. 1-21. https://doi.org/10.22367/jem.2021.43.01.

Mackay, D. 2017. Blog text. "Technology and GDPR: Is your platform ready?" *ITProPortal,* 24.10.2017 Retrieved 8.3.2022 from https://www.itproportal.com/features/technology-and-gdpr-is-your-platform-ready/.

Monteiro-Krebs, L., Rodriguez, O.L.A., Dewitte, P., Ausloos, J., Geerts, D., Naudts, L., and Verbert, K. 2019. "Tell Me What You Know: GDPR Implications on Designing Transparency and Accountability for News Recommender Systems", in *CHI 2019,* Glasgow.

Nabbosa, V. and Iftikhar, R. 2019. "Digital Retail Challenges within the EU: Fulfillment of Holistic Customer Journey Post GDPR", in *Proceedings of the 2019 3rd International Conference on E-Education, E-Business and E-Technology*, pp. 51-58. https://doi.org/10.1145/3355166.3355170.

Pandit, H.J. and Lewis.D. 2018. "Ease and Ethics of User Profiling in Black Mirror", *in WWW '18 Companion: The 2018 Web Conference Companion*, April 23–27, 2018, Lyon, France. ACM, New York, NY, USA, https://doi.org/10.1145/3184558.3191614 .

Paré, G., Tate, M., Johnstone, D. and Kitsiou, S. 2016. "Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews", in *European Journal of Information Systems* (25:6), pp. 493–508.

Povse, D.F. 2018. "It's all fun and games, and some legalese: Data protection implications for increasing cyber-skills of employees through games", in *Proceedings of Central European Cybersecurity Conference* (Ljubljana '18). https://doi.org/10.1145/3277570.3277580.

Raponi, S. and Pietro, D. 2020. "A Longitudinal Study on Web-Sites Password Management (in)Security: Evidence and Remedies", in *IEEE Access,* (8), pp. 52075-52090, 2020. 10.1109/ACCESS.2020.2981207.

Rowe, F. 2014. "What literature review is not: Diversity, boundaries and recommendations", in *European Journal of Information Systems* (23:3), pp. 241–255.

Sağlam, R. and Nurse, J. 2020. *Is your chatbot GDPR compliant? Open issues in agent design*. 10.1145/3405755.3406131.

Sailaja, N., Crabtree, A., McAuley, D. and Stenton, P. 2018." Explicating the Challenges of Providing Novel Media Experiences Driven by User Personal Data", in *Proceedings of the 2018 ACM International Conference on Interactive Experiences for TV and Online Video* (TVX '18). Association for Computing Machinery, New York, NY, USA, pp. 101–113. https://doi.org/10.1145/3210825.3210830.

Sánchez-Monedero, J. Dencik, L. and Edwards, L. 2020. "What does it mean to 'solve' the problem of discrimination in hiring?: social, technical and legal perspectives from the UK on automated hiring systems", in *SSRN Electronic Journal*, pp. 458-468. https://doi.org/10.1145/3351095.3372849.

Sanchez-Rola, I.,Dell'Amico,M., Kotzias,P., Balzarotti, D., Bilge,L., Vervier,P.A. and Santos, I. 2019. "Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control", in *ACM Asia Conference on Computer and Communications Security* (AsiaCCS '19), July 9– 12, 2019, Auckland, New Zealand. ACM, New York, NY, USA. https://doi.org/10.1145/3321705.3329806 .

Schryen, G. 2015. "Writing qualitative IS literature reviews—guidelines for synthesis, interpretation, and guidance of research", in *Communications of the Association for Information Systems* (37-12), pp. 286–325.

Seo, J., Kim, K., Park, M., Park, M. and Lee, K. (2017). "An analysis of economic impact on IoT under GDPR", in *8th International Conference on Information and Communication Technology Convergence* (ICTC), Korea, pp. 879-881, https://doi.org/10.1109/ICTC.2017.8190804.

Shastri, S., Banakar, V., Wasserman, M., Kumar, A. and Chidambaram, V. 2020. "Understanding and benchmarking the impact of GDPR on database systems", in *Proceedings of the VLDB Endowment*. (13), pp. 1064-1077. https://doi.org/10.14778/3384345.3384354.

Sobers, R. 2018. *The average reading level of a privacy policy*. https://www.varonis.com/blog/gdpr-privacy-policy/.

Sirur S., Nurse, J. and Webb H. 2018. "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)", in *25th ACM Conference on Computer and Communication Security*, Canada, pp. 1-8.

Snyder, H. 2019. "Literature review as a research methodology: An overview and guidelines", in *Journal of Business Research*, (104), pp. 333-339, ISSN 0148 -2963, https://doi.org/10.1016/j.jbusres.2019.07.039.

Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T. and Klepacki, B. 2019. "Information Security Assessment in Public Administration", in *Computers & Security*. 90. 101709. 10.1016/j.cose.2019.101709.

Tankard, C. 2016. "What the GDPR means for businesses*", in Network Security*, (2016:6), pp. 5-8.

Tatara, U., Gokceb, Y., and Nussbaum, B. 2020. "Law versus technology: Blockchain, GDPR, and tough tradeoffs", in *Computer Law & Security Review*, (38), Article 105454. https://doi.org/10.1016/j.clsr.2020.105454.

Teixeira, G., Mira da Silva, M. and Pereira, R. 2019. "The critical success factors of GDPR implementation - a systematic literature review", in *Digital Policy, Regulation and Governance*. (21:4), pp. 402-418.

The University of Alberta. 2022. *Research methods Lessons 2*. Retrieved 28.2.2022 from: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fsites.ualberta.ca%2F~carmen%2F325a1%2FResearch%2520MethodsLesson2.ppt&wdOrigin=BROWSELINK.

Urban, T., Degeling, M., Holz, T. and Pohlmann, N. 2019. ""Your Hashed IP Address: Ubuntu." - Perspectives on Transparency Tools for Online Advertising", in *Annual Computer Security Applications Conference*. San Juan, Puerto Rico. https://doi.org/10.1145/3359789.3359798.

Utz, C., Degeling, M.,Fahl, S.,Schaub, F. and Holz, T. 2019. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *ACM SIGSAC Conference on Computer and Communications Security* (CCS'19).10.1145/3319535.3354212.

Vimercati, S.D., Foresti, S., Livraga, G., and Samarati, P. 2012. "Data Privacy: Definitions and Techniques", in *Int. J. Uncertain.* Fuzziness Knowl. Based Syst., (20), pp. 793-818.

Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B. and Plattfaut, R. 2015."Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research", in *Communications of the Association for Information Systems* (37:9), pp. 205–224.

Zou, Y., Danino, S., Sun, K. and Schaub, F. 2019. "You 'Might' Be Afected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifcations", in *CHI Conference on Human Factors in Computing Systems Proceedings* (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK. ACM, New York, NY, USA, https://doi.org/10.1145/3290605.3300424

Wallace, N. and Castro, D. 2018. *The impact of the EU's new data protection regulation on AI*. Retrieved from https://www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/

Webster, J., and Watson, R.T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review", in *MIS Quarterly* (26:2), pp iii-xiii-

Whitman, M.E. and Mattord. H.J. 2011. *Principles of information security*. Cengage Learning.

Withey, V. 2018. *The impact of GDPR on the technology sector*. Retrieved 12.1.2022 from https://gdpr.report/news/2018/03/19/the-impact-of-gdpr-on-the-technology-sector/