Organisational GDPR Investments and Impacts

Pauliina Hirvonen
University of Jyväskylä, Jyväskylä, Finland

pauliina.a.hirvonen@student.jyu.fi

Abstract: The aim of this empirical multi-case study is to understand the GDPR investments and impacts of the organisations. Among these, the measuring experiences related to GDPR and information security (Isec), and the future expectations are examined. Several interesting findings were recognised, which also enabled further suggestions. First, an understanding of the organisations' investments and their impact is built by gathering information about the actions that organisations made to fulfil the GDPR requirements. In the second phase, it is deemed necessary to examine how organisations experience the measures and evaluation of GDPR development and progress, in order to understand how respondents, end up evaluating the impact of their investments. In the third phase it is considered necessary to consider the future development of GDPR and the challenges and opportunities it brings to organisations, in order to understand how the experiences so far affect preparations for the future. The final phase of evaluation focuses on finding out what impact the GDPR has had on organisations. On the one hand, it is possible that the total investment in the GDPR may also correlate with the development of the organisational Isec maturity, because GDPR has brought more resources and visibility to the organisation's Isec, and operations have become more systematic. On the other hand, organisations with an already high level of Isec maturity and organisations operating in a regulatory-focused industry may accept the GDPR-based Isec investments more easily. If GDPR is tightly integrated with both the organisation's information security and the business functions under the responsibility of executive management, it may support the organisation's business and information security development. This research serves GDPR authorities, organisational executives, persons in charge of GDPR/information security/cybersecurity, service providers and academia.

Keywords: GDPR investments, Empirical GDPR research, Organisational GDPR impacts, Privacy impacts, Information security development, Privacy development assessment

1. Introduction

General Data Protection Regulation (GDPR) brought opportunities in many areas of everyday life for European citizens, technology organisations and different businesses, but also unwanted challenges and interpretation complexities (Tene et al., 2019). As previous research was not able to look at the phenomenon holistically, the aim of this research was to understand comprehensively what GDPR has demanded and caused. The main research question for the multi-case study was: what are the organisational efforts for GDPR and how has GDPR impacted the organisational information security (Isec)? In this research, *the investments concept* refers to all tangible and intangible input, workload, and efforts the organisation has made to meet GDPR requirements. Investment types are treated in this study as qualitative units, and not as precise quantitative measures. *The impacts of GDPR* refer to all the consequences that the regulation has caused for organisations.

The research issue is approached through a multi-case study consisting of eight cases as the eight separate companies. Research aspects included providing several conclusions related to organisations' experiences in GDPR resourcing and measuring organisational Isec development, expectations for future GDPR development and the various impacts of GDPR are made. Suggestions for practices and future research are proposed as well. This research serves GDPR authorities, organisational executives, persons in charge of GDPR/information security/cybersecurity, ICT/ISEC-service providers and academia. The research is organised as follows: Section 2 discusses previous research. The methodology is presented in Section 3. Section 4 includes the analysis. The discussion is in Section 5 and, finally, the conclusions are presented in Section 6.

2. Previous Research

The purpose of reviewing previous research is not to unpack the GDPR articles or requirements in detail, but to understand existing aspects related to organisational GDPR experiences. Perspectives of GDPR efforts and resourcing were found for example by Dibble (2020), who investigated that, instead of being just a once-off exercise, GDPR is more about developing a pervasive framework to cherish the privacy culture. Dode (2018) noted the challenge of correct interpretation and legal interpretation of GDPR requirements. Politou et al. (2018) described the challenge of GDPR for compliance development as containing a restricted number of technical implementation instructions. Tikkinen-Piri et al. (2018) estimated GDPR to require remarkable financial and

human resources and employee training. Degeling et al. (2019) noticed that ICT companies moved in phases to GDPR rather than creating new approaches in their system architecture for GDPR compliance. Dode (2018) mentioned significant requirements for ICT planning and data storage and lineage due to GDPR legal function and compliance. Li et al. (2019) also stated that, organisations must invest, particularly in manpower and resources, to evaluate, develop and redesign their technology platforms and data architectures, update data protection (DP) policies, change advertising policies and adjust data storage and processes.

Most of the research discussed GDPR impacts. Several research (e.g., Poritskiy et al., 2019; Politou et al., 2019; Dellei, 2009) recognised increased confidence and clarifications as the main benefits of GDPR. Poritskiy et al. (2019) identified that organisations experienced hard times with GDPR requirements, especially with the execution of system and process audits and the application of the right to erasure. This survey (Poritskiey et al., 2019) also indicated that the state of implementation of GDPR and the company type are important factors impacting on how GDPR benefits and challenges are perceived. Also the size of the organisation seemed to matter on GDPR impacts (see for example Phillips, 2019; Politou et al., 2019; Bershidsky, 2018 and Goddard, 2017). Li et al. (2019) noted that GDPR complicates the operations of organisations, limits their scope and increases operating costs, which subsequently hampers the productivity and effectiveness of these emerging technologies. Tsohou et al. (2020) noticed that privacy, security, legal and technology acceptance became visible and then integrated GDPR compliance platform requirements. Jia et al. (2018) found negative GDPR impacts on technology investment appearing, particularly for nascent ventures (0 – 3 years) compared to their US counterparts. Impacts are also considered from many other technological aspects (see Wallace and Castro, 2018; Mackay, 2017; Greengard; 2018; and Nautsch et al., 2019).

It is clear that the GDPR is very likely to have an impact on organisational Isec and cyber security (Csec) aspects as GDPR Article 5 imposes regulations on these matters. For example, Mikkelsen et al. (2019) estimated that the investment falls on security controls, continued investments in Csec, and improving internal processes since organisations have to automate and streamline to meet the GDPR requirements. Layton and Elaluf-Claderwood (2019) reported that organisations are faced with remarkable investment costs, especially on privacy compliance. Bilyk (2018) shared ITC companies' challenges to build applications that use personal data in technical and organisational environments. Krikke et al. (2019) explained privacy-by-design to support ICT companies to develop better security solutions, while Fimin (2018) and Bennett (2018) revealed GDPR to improve data management process.

As review shows, the GDPR resourcing and impacts have been examined from several specific perspectives. However, most of the previous research lacked approaching resourcing and impacts comprehensively. All four aspects, including efforts and impacts, measuring the GDPR/Isec development through GDPR efforts, and future expectations of GDPR were not combined in previous research. Empirical research located in Northern Europe was also limited. This research filled the gap by recognising factors related to phenomena based on experiences of eight companies.

3. Methodology and Research Implementation

This research was a multi-case study consisting of eight cases as the eight separate companies and the research aspect as the GDPR impact phenomena examined within each case. Gustafsson (2017) explained the necessity for a multi-case study, when there is more than one single case and, as Eisenhardt and Graebner (2007) described, there is a need for wider exploration of research questions to build more convincing results. The research aspect included four sub-aspects. The research aspect and the main research questions per sub-aspects are presented in Table 1.

Table 1. **Research Aspect and Sub-aspects of the Multi-case Study**

Research aspect	Research sub-aspect	Research question
Organisational GDPR Investments and Impacts	Organisational Investments and Efforts	What has been invested in GDPR in the organisation?
	Measuring Organisational GDPR and Isec Development	How are the development of GDPR /Isec evaluated and what are the main conclusions of the development?
	Future Expectations and Costs	What are future expectations of GDPR and what does it demand from organisations?
	GDPR Impacts	What are the GDPR impacts for the organisation?

Eight interviews were conducted by the author in eight medium or large sized Finnish companies in the autumn in 2021. Each research sub-aspect contained several open-ended interview questions. The industry types were energy, media, engineering, retailing, construction, and software. 1 - 3 participants were interviewed for each organisation. The interviewees worked in varying roles and were persons in charge of GDPR in companies.

Qualitative approach is suitable for research where the examination of the phenomenon is based on subjective experiences without unambiguous truth (Paley, 2000). An advantage of the qualitative multi-case study approach is also that the researcher may refer to the similarities and differences between different cases in a multi-case study, when compared to one case study. This was done by using explanation building techniques together with cross-case comparisons and theming as an analysing method. The data was coded inductively. The thematic analysis increased the relevant content of all results data and supported to find the connections of the interferences of the different approaches in and between cases.

4. Analysis of the Results

The main research question examined what the organisational efforts for GDPR are and how has GDPR impacted the organisational information security (Isec). As noted in Introduction section, the investment types are treated here as qualitative units, and not as precise quantitative measures. The analysis of the results were built in four phases. First, an understanding of the organisations' investments and their impact was built by gathering information about the actions that organisations made to fulfil the GDPR requirements. Next step included examining how organisations measure GDPR and its connection to Isec development. In the third phase the future development of GDPR was considered. The final phase observed what impact the GDPR has had on organisations.

1) Organisational Investment and Efforts for GDPR

GDPR investments were intangible and tangible, direct but also indirect (would have taken place without GDPR). Some investments were non-recurring, for example, system investments, and some were ongoing activities, such as training. *Investment types were identified in seven different areas: management, human resources, finance, organisational change, operational processes, ICT and cooperation*. The results showed that the main effort required human resources (working time). The GDPR was promoted in many organisations in the same way as other development projects, and experts are involved where appropriate. Permissions and resources related to the most significant investments and development were sought from the executive management (EM) , but training and practical compliance were typically decided at the DP organisation level. Three effective means were mentioned to support acceptance of GDPR investment proposals: 1) invoking the content of the regulation, 2) a risk assessment (what would the impact be if there were no change), and 3) an organisational continuity management/development perspective. Decisions related to the fulfilment of the minimum GDPR requirements, decisions that can be economically justified, and decisions that do not incur costs were considered straightforward.

The most challenging decisions mainly concerned upgrades to existing systems or ICT solutions that otherwise contained differences of interpretation. For the most challenging or employable GDPR investment ranged from individual activities to the overall implementation of the GDPR. Four responses emphasised the specific challenges relating to the initial phase, when the content of the requirements was not entirely clear due to a lack of official guidance information. The mapping of the location of personal data, impact assessment, execution of requests for personal data, system investments and "kneading" staff in GDPR matters were also mentioned as the single most challenging aspects. Also, overall compliance and, for example, changing the organisation's operating models and cooperating with partners outside the EU, was seen as confusing according to two companies. The responses revealed differences in the assessment of the significance of the total investment. The total investment was estimated to be important for the organisation (externally reliable player, business development, DP-focused contract expertise management) according to five responses. *The nature of the operations of the organisations also determined how much the investment was seen to benefit the business*. GDPR was mostly seen as an ongoing process rather than a one-time performance.

2) Measuring Organisational GDPR and Isec Development

The impact of GDPR on the specific areas of Isec development and ways to evaluate it in organisations have been varied. All (8/8) companies however agreed that GDPR has had a positive influence on Isec development. The

majority (6/8) of interviewees agreed that GDPR and impact assessment expertise due to training and testing, agreements with partners at various levels of the organisation have brought more resources and visibility to the organisation's Isec and that operations have become more systematic, meaning an increase in Isec training, instruction, testing and preparedness in many organisations. GDPR has improved Isec, but also indirectly Csec and overall security maturity in the organisations 3/8), and intensified cooperation between these functions in organisations (5/8). For two organisations, GDPR and Isec together have enhanced or created a new business opportunity for responsibility. In many organisations (6/8) , DP and Isec were separate operations, although they were implemented in parallel, but *strengthening the dialogue between GDPR, Isec and business perspectives was mentioned as a success factor of organisational development*. Isec has been essential in the construction and maintenance of GDPR compliance, particularly through technical Isec system solutions. In three organisations, Isec is an interpreter between the implementation of GDPR requirements and ICT solutions. Isec and Csec were in some organisations completely reorganised, helped by GDPR. Based on the analysis of the responses it was found that *organisations with a high level of Isec maturity and organisations operating in a regulatory-focused industry were associated with a more flexible acceptance of GDPR-based Isec investments proposals.* However, the development of Isec has, from a GDPR perspective, mainly meant raising awareness of the risks involved in everyday life and operations and updating or acquiring technical Isec solutions. Isec investments (e.g., control) may also still have negative costs for some organisations. In particular, five arguments proved to be essential to GDPR-related Isec investment proposal acceptance (e.g., purchase of a service) in organisations: business continuity, raising the level of the SA of the Isec, risk assessment, importance of reputation and financial threat.

A significant part of GDPR development assessment in every company came from internal feedback and questions, and training evaluations. The interviewees mentioned the following activities: monitoring of DP reporting in internal reporting, evaluation of training and training volumes, analysis of the number and quality of personal data requests, process control, analysis of the number and quality of data breaches, internal contacts, feedback and questions, reviewing DP and Isec status of new parts and functions of the organisation (e.g., after the expansion of the organisation). Organisations may also rely on external auditors to assess Isec development.

3) Future Expectations

With regard to the further development of the GDPR, it was hoped that all the legal demands that organisations should take into account, for example, marketing data, would be covered under one piece of legislation. In addition, timely, unambiguous, detailed and practical industry-specific guidance (e.g., industry-specific checklists) was requested. In particular, guidance on the automation implementation of e-privacy regulation, the formation of DP organisations, and effective tools and clear guidelines for impact assessment were sought. It was hoped that GDPR oversight would take into account the size and industry of organisations and degree of sensitivity to personal information. In addition to fines, it was seen as necessary for the GDPR authorities to provide tools to solve the problems. The specific national issues and the impact of Brexit were seen as a challenge for the future. Experience to date with the GDPR has shown organisations in particular the need to take into account the flexibility of change in all activities of the organisation, the need to identify the location of personal data in the organisation and to take DP into account in the development of new business. The most significant challenges for the future GDPR implementation were data management, contract negotiations for the processing of personal data across EU borders, identification of regulations binding the organisation, delays in guidance issued by regulatory authorities, new solutions requiring evaluation, partnership agreements and changes in the organisation's operations as a result of Brexit.

The most significant development needs of GDPR authorities in the future were the clarification of steering roles and the development of frontloading, improving the clarity and concreteness of instructions, concentrating supervision on GDPR-sensitive organisations and addressing GDPR-induced inequality in the competitive field. The authorities were expected to make the DP management systems available for organisations. In particular, EU-level authorities were requested to have more capacity for a faster cycle of processing decisions, guidelines and recommendations.

4) GDPR Impacts on Organisations

The results showed that the GDPR impacts were generally assessed by most to be significant, pervasive, and lasting. Impacts were seen to be both internal and external (e.g., customers). Some positive impacts are:

responsibilities and accountability, growing importance of partnership agreements, strengthening GDPR awareness and compliance (requirements and guidelines), developing and increasing operating models and processes, access to systems, development of Isec and Csec and overall security guidelines, improved transparency for customers and organisational development of responsibility. The negative effects of GDPR were seen as ongoing resourcing needs (people, money, management) required to maintain compliance in organisations. GDPR was found to be labour intensive for non-personally sensitive organisations. It was noted that bureaucracy related to official guidance increased.

The most significant effects mentioned were the development of the organisation's DP culture and awareness, the benefits for organisational investments in general, as well as the improvement in customer confidence, the decrease in the response time of one's own service and the increase in system knowledge. Although the GDPR process has been a challenging and complex entity for most, organisations managed to evaluate, prepare and adapt to GDPR requirements and to anticipate the effects on organisations, which helped to reduce unexpected or false effects on a wider scale. The small number of requests for personal information or action were the most unexpected positive effects according to four companies. Three interviewees were also surprised by the lack of control and sanction by the official GDPR governing bodies. According to the results, the GDPR did not bring any new competence requirements, but rather changes in small practices. The key GDPR competency requirements related to the following areas:

- Knowledge Of The GDPR Content
- Interpretation And Applications
- Contract Negotiation
- Staff Engagement
- GDPR, Isec And Csec Integration
- Training And Development
- Raising Of Organisational GDPR Situational Awareness (SA)
- Knowledge And Awareness Of Organisation
- Competency Mapping
- Personal Data Process Management
- Project Management

When asked about the overall success of the GDPR, it was mentioned that the goal of the GDPR has been successful and the GDPR was seen to have raised society's DP awareness internationally and Isec expertise of Finnish society. It was mentioned that the GDPR has brought DP cases to industries it had not previously touched on and brought deeper understanding to DP control and the threat of sanctions, but the definition of data breach should be clarified. For the authorities, there was also a need to reduce the response delay and they were encouraged to consider the sector, size and GDPR sensitivity of the organisation. It was mentioned by the majority of the companies (5/8), that the lack of guidance from the official GDPR has had a wide impact on some organisations and that the implementation of the GDPR in organisations would have been more controlled, coherent and streamlined if clear official guidance on requirements had been provided on time.

5. Discussion, Implication for Practices and Restrictions

The result highlighted that the GDPR has required (and still requires) a significant amount of tangible and intangible investments and resources. Totally investments related to seven different areas were identified. GDPR has had a real impact on the development of information security in most of the examined organisations. Some organisations, especially ones with lower maturity levels of Isec, may still find it challenging to justify investment needs to the decision-makers. Organisations with an already high level of Isec maturity and organisations operating in a regulatory-focused industry may accept the GDPR-based Isec investments proposals more easily. However, the practices found to be successful for achieving investment decision approval were shared in this research. As a cross-cutting ongoing process for an organisation, GDPR, if closely integrated with both the organisation's information security and the business functions under the responsibility of EM, may support the organisation's business development and information security development.

Based on the analysis, it is possible that the total investment in the GDPR may also correlate with the development of the organisational Isec maturity and indirectly support the development of Csec and overall security, because GDPR has brought more resources and visibility to the organisation's Isec, and that operations

have become more systematic. As noted in the analysis, GDPR and Isec together have created a new business opportunity for responsibility and it is suggested that organisations enhance the development of GDPR, Isec, Csec and overall security at the same, integrating all these aspects into business functions in every level of the organisations. Practically, this may happen by increasing DP awareness and increasing impact assessment expertise through guidance, training and testing. Also, through agreements with partners at various levels of the organisation, procurement, system upgrades, developments, Isec tools and practices may support the integration. This kind of approach may also support faster integration of information security into all activities of the organisation. However, it seems that organisations still have a long way to go in turning GDPR into business opportunities by themselves.

Related to challenges experienced with the GDPR: legacy systems, system upgrades/integrations or acquisition, ICT and Isec companies could support organisations to balance optimal solutions and also integrate the DP and Isec activities more effectively. To support organisations to deal with future GDPR developments, including development assessment, it is suggested that the GDPR authorities provide certification of standardisation that may help organisations to select appropriate and verified tools, consultants, partners and service providers. The future GDPR challenges relate to the guidance for implementation of automation, e-privacy regulation, the DP organisation development, guidelines and tools for impact assessment and data management, contract negotiations for the data processing across EU borders, partnership agreements, Brexit impact assessment and getting reliable guidance and decisions from officials without delay. GDPR authorities' resources may be used more efficiently by shifting the focus towards the following areas: the clarification of steering roles, the development of frontloading, improving the clarity and concreteness of instructions, concentrating supervision on GDPR-sensitive organisations and addressing GDPR-induced inequality in the competitive field. When comparing these observations of GDPR challenges to research of Poritskiy et al. (2019), two aspects did not come up in the interviews, namely limits the growth of emergent technologies and increasing technical complexity. However, two aspects classified as challenges by Poritskiy et al. (2019), namely employee training and increasing budget associated with security operations, emerged here in the interview as positive or neutral effects.

The major implications in Isec development are the development of the organisation's DP culture and awareness, benefits for the organisational investments in general and improved customer confidence, decrease of response time of own services and increased system knowledge. The data management, opposite to Poritskiy et al. (2018), was seen here as a challenge. As known publicly, there is a huge annual increase in the amount of data as technology advances and expands. For example, only in Finland, between 2019 and 2020, the amount of data increased by about 19% per year (Finnish Federation for Communications and Teleinformatics, 2022). Organisations outside the ICT may consider data management challenging.

These findings can provide interesting insights, especially for official GDPR authorities and law developers, as the results provide observations and recommendations not only from an organisational perspective, but from a more holistic point of view. At the same time, the results serve as authentic feedback on the experiences of medium-sized and large organisations in implementing GDPR during 2018-2021, which can help authorities to improve communication towards organisations and to improve the quality of guidance and information. It is hoped that the results will have a particular impact on organisations' operations and facilitate the implementation of the GDPR and related laws. For EM), the results also show that the organisation's business and its development can successfully be integrated with GDPR, Isec/Csec and the development of overall security, and that they must have an ongoing active and open dialogue in the day-to-day life of the organisation. It may also be useful both for EM and DP organisations to understand the challenges and opportunities associated with GDPR investment. As the results showed the EM's support and commitment to GDPR are critical to achieve GDPR compliance in the organisation. Results may activate and innovate service and solutions providers and ICT, Isec and Csec companies to apply the findings in DP, Isec and Csec product and service design, and support requirement specification and intensify communication with organisations. For external partners, the study will provide detailed information of the content and the timing of the support needs, so the services can be targeted optimally. Research also included suggestions for further academic empirical research, as it touches the surface of several significant GDPR subject areas.

5.1 Restrictions and Future Study

As usual, the most common restriction of the case study research relates to the lack of generalisability of the research results. The research data, consisting of interviews, are subjective, as well as the analysis of the findings, because it is based on the experiences of individuals.

Future research is needed to gain a more comprehensive perspective of this wide research issue. It is recommended to explore the issue by using different research strategies, approaches and methods, but also taking a wider set of samples, and expanding the scope to other EU countries or outside EU borders. Also, as the GDPR landscape is changing, conducting follow-up studies would help to assess long-term effects.

6. Conclusions

A multi-case study consisting of eight cases as the eight Finnish companies was conducted to explore the GDPR experiences in organisations. This research complemented existing and found new perspectives for the issue. The research questions of the multi-case study explored what GDPR has demanded and caused for organisations. The answers to all four research sub-aspects were found and several inferences related to organisations' experiences of GDPR resourcing, measuring GDPR and Isec development, expectations of the future development of the GDPR and the variable implications of GDPR were made. Investments related to seven different areas were identified. It is possible that the total investment in the GDPR may also correlate with the development of the organisational Isec maturity, because GDPR has brought more resources and visibility to the organisation's Isec, and operations have become more systematic. However, organisations with an already high Isec level of maturity, and organisations operating in a regulatory-focused industry, may accept the GDPR-based Isec investments more easily. As a cross-cutting ongoing process for an organisation, GDPR, if closely integrated with both the organisation's information security and the business functions under the responsibility of EM, supports the organisation's business development and information security development. Besides several positive effects, the initial phase of implementation in particular was perceived as very challenging due to unclear communication from the GDPR authorities. Research included suggestions for practices and future research. This research is hoped to serve several parties working with GDPR: authorities, organisational executives, persons in charge of GDPR, ICT/ISEC service providers and academia.

References

Bennett, C. (2018). The European general data protection regulation: an instrument for the globalization of privacy standards? *Information Policy*, 23(2), pp. 239-246.

Bershidsky, L. (2018). *Europe's privacy rules are having unintended consequences.* www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are

Bilyk, V. (2018). *Challenges and benefits of GDPR implementation.* https://theappsolutions. com/blog/development/gdpr-challenges-and-benefits/

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy...now take some cookies: measuring the GDPR's impact on web privacy. *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2019*, San Diego, CA, pp. 1-15.

Dellei, L. (2019). *GDPR compliance as a competitive advantage.* www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?List = ef7cbc6d-9997-4b62-96a4-a36fb7e171af&ID=1133&utm_referrer=direct%2Fnot%20provided

Dibble, S. (2020). The GDPR Marathon. *Solicitors journal,* 163(3), p. 40.

Dode, A. (2018). The challenges of implementing General Data Protection Law (GDPR). *14th International Conference in "Standardization, protypes and quality: a means of Balkan countries' collaboration*", September 21 - 22, 2018, Tirana, Albania. https://www.researchgate.net/profile/Albi-Dode/publication/327829348_The_challenges_of_implementing_General_Data_Protection_Law_GDPR/links/5ba74542299bf13e6045fca9/The-challenges-of-implementing-General-Data-Protection-Law-GDPR.pdf

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *The Academy of Management Journal,* (50:1), pp. 25-32.

Finnish Federation for Communications and Teleinformatics. (2022). Matkaviestinverkossa siirretty data.https://www.ficom.fi/ict-ala/tietopankki/viestintaverkot-tietopankki/kiintea-ja-mobiililaajakaista/matkaviestinverkossa-siirretty-dat/

Fimin, M. (2018). *Five benefits GDPR compliance will bring to your business*. www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your business/#1d2981cb482f

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

Greengard, S. (2018). Weighing the Impact of GDPR. *Communications of the ACM* (61:11). Society. News. DOI:10.1145/3276744

Gustafsson, J. (2017). *Single case studies vs. multiple case studies: A comparative study.*

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

Jia, J., Jin, G. Z., and Wagman, L. (2018). *The short-run effects of GDPR on technology venture investment* (No. w25248). National Bureau of Economic Research.

Krikke, J., Valgaeren, E., and Origer, G. (2019). *Complying with the general data protection regulation* (GDPR). NBER Working Paper No. 25248. November 2018. JEL No. D43,D8,L13,L15,L5. www.stibbe.com/en/expertise/practiceareas/data-protection/general-dataprotection regulation/what-are-the-challenges

Layton, R., and Elaluf-Calderwood, S. (2019). A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices. *12th CMI Conference on Cybersecurity and Privacy* (CMI), pp. 1-6. doi: 10.1109/CMI48017.2019.8962288.

Mackay, D. (2017). *The impact of GDPR from a technology perspective – is your platform ready?* https://www.ness.com/11101-2/

Mikkelsen, D., Soller, H., Strandell-Jansson, M., and Wahlers, M. (2019). *GDPR compliance since May 2018: A continuing challenge*. Risk Practice. McKinsey & Company. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/GDPR%20compliance%20after%20May%202018%20A%20continuing%20challenge/GDPR-compliance-since-May-2018-A-continuing-challenge.pdf

Nautsch, A., Jasserand, C., Kindt, E., Todisco, M., Trancoso, I., & Evans, N. (2019). The GDPR & Speech Data: Reflections of Legal and Technology Communities, First Steps towards a Common Understanding. Proc. *Interspeech 2019*. https://doi.org/10.48550/arXiv.1907.03458

Paley, J. M. A. (2000). Paradigms and presuppositions: The difference between qualitative and quantitative research. *Scholarly Inquiry for Nursing Practice,* (14:2), pp. 143-155. https://www.proquest.com/scholarly-journals/paradigms-presuppositions-difference-between/docview/893000198/se-2?accountid=11774

Phillips, N. (2019). Keep it: Maintaining competition in the privacy debate. Remarks for Internet Governance Forum.

Politou, E., Alepis, E., and Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, (4:1). https://doi.org/10.1093/cybsec/tyy001

Politou, E., Michota, A., Alepis, E., Pocs, M., and Patsakis, C. (2019). Backups and the right to be forgotten in the GDPR: an uneasy relationship. *Computer Law & Security Review,* (34:6), pp. 1247-1257.

Poritskiy, N., Oliveira, F., and Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, (21:5), pp. 510-524. doi:http://dx.doi.org/10.1108/DPRG-05-2019-0039

Tene, O., Evans, K., Gencarelli, B., Maldoff, G., and Zanfir-Fortuna, G. (2019). GDPR at Year One: Enter the Designers and Engineers. *IEEE Security & Privacy*, (17), pp. 7-9. 10.1109/MSEC.2019.2938196.

Tikkinen-Piri, C., Rohunen, A., and Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies*. Computer Law & Security Review*, (34:1), pp. 134-153.

Tsohou, A., Magkos, E., Mouratidis, H., et al. (2020). Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. *Information & Computer Security.*

Wallace, N., & Castro, D. (2018). *The impact of the EU's new data protection regulation on AI.* www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulationon-ai/