Building Situational Awareness of GDPR

Pauliina Hirvonen and Martti J. Kari
University of Jyväskylä, Finland

pauliina.a.hirvonen@student.jyu.fi
martti.j.kari@jyu.fi

Abstract: Because previous academic research does not comment sufficiently on how the relevant content of the European Union (EU) General Data Protection Regulation (GDPR has been properly communicated to the organisations, or how the situational awareness (SA) of GDPR has been built in the organisations, this qualitative empirical research was regarded as a valuable approach for gathering authentic research material on the practical bases of this phenomena. The aim of this empirical case study (CS) is to develop a picture of what processes organisations use to build SA of the GDPR requirements. To guide the CS, we asked how the SA for decision-making was constructed and how it was perceived in organisations. The experiences of eight Finnish organisations showed that the organisations' practices of building SA and their experiences with the quality and adequacy of SA differed. However, building SA proved to be a critical step for organisations in the overall process of meeting GDPR requirements. Especially the data coming from inside the organisation became very relevant in the SA process, because it supported decision makers to determine how the GDPR requirements should be implemented in the organisation. As a main contribution of this article, based on best practices shared by organisations a model of building SA was built. The proposed model is threefold and was constructed by combining the findings of an empirical CS analysis, the steps of the intelligence process, and the essential elements of the model of creating information security SA. The result is potentially beneficial for building situational understanding of any complex or ambiguous issue, especially in complex and digitalised technological areas, where combining information management with accurate and efficient decision-making is a common challenge. The results can be used by any party who is looking to build SA of an abstract issue in a complex environment.

Keywords: GDPR requirements, Interpreting privacy regulation, Understanding GDPR requirements, Organisational situational awareness, Privacy practices, Information security development

1. Introduction

Previous research does not comment sufficiently on how the relevant content of the European Union (EU) General Data Protection Regulation (GDPR) has been properly communicated to the organisations, or how the situational awareness (SA) of GDPR has been built in the organisations. As, for example, Ahmad et al. (2021) stated, most research has focused more on technological than practical perspectives. The development history of the research topic has been significantly influenced by the need to produce practical research information on GDPR issues in academic research, which can support the environment, for example service providers or legislators to develop usable solutions for organisations that facilitate the implementation of privacy, for example GDPR issues. GDPR was perceived by organisations as impractical and challenging from the start (see e.g. Tankard, 2016; Sirur et al, 2018; Hirvonen, 2022a and 2022b), so clarifying solutions and a model are needed to improve developing GDPR SA. The research data for this case study was already collected in 2021, so more scientific research on the topic has naturally been published after that. However, it can be stated that even after 2021, research progress does not concentrate only on the privacy side, but more broadly on e.g. cyber security, although even these solutions can be seen to benefit the privacy side as well.

The aim of this case study (CS) is to develop an overall picture of how organisations build SA of GDPR requirements. The objectives are 1) to collect practices found to be working by organisations, and 2) based on these to provide a model with which other organisations can facilitate when creating the SA. The research question is: How was the SA for decision-making constructed and how was it perceived within the organisation?

The concept of SA has several definitions. According to Tikanmäki and Ruoslahti (2019), all SA definitions share the idea of knowing and understanding what is occurring, prediction of the future situation, and the decision-making based on these factors. In this study, SA means the organisational awareness of all the actions, decisions, expenditures, resources, investments and mindsets required to demonstrate GDPR compliance in practice. SA also essentially involves an understanding of the changes in future needs of the organisation, the environment and GDPR. Organisations use their SA as the basis for decisions about the activities and resources related to GDPR.

The results here indicate that organisations' practices for building SA and their experiences of its quality and adequacy differed. However, building SA proved to be a critical step for organisations in the overall process of

meeting GDPR requirements, because decisions on the necessary actions and investments are made based on SA. Using these results, necessary parts for building a model of building optimal SA for organisational decision-making is gathered. This research of building SA of GDPR has the following structure: the highlights of existing literature are introduced in Section 2, the methodological choices are shortly described in Section 3. The results and analysis are presented in Section 4. The discussion is in Section 5. Finally, the conclusions are located in Section 6.

2. Early Work

Quite a limited amount of research of what is already known about building the SA, concentrating specifically on the GDPR or data protection (DP) requirements approach, was found. For example, Teixeira et al. (2019) acknowledged the importance of regulation awareness in organisations, including requirements and obligations. Their review, which examined the success factors of GDPR implementation, was the most complete research of the ones discussed here, because it highlighted research issues comprehensively, contributing the identification of enablers, benefits, challenges and the barriers affecting the compliance process. Aberkane et al. (2021) investigated the consideration of the GDPR regulation when developing service solutions in organisations. Organisations' challenges with interpreting GDPR have been reported by Tankard (2016) and Sirur et al. (2018). As also the empirical evidence demonstrated that in 2018 more than 50% of all websites failed to present privacy policies for consumers in an adequate manner (Dellinger, 2019). Seo et al. (2017) warned of forthcoming challenges due to the GDPR for organisations that process large amounts of personal data. Capgemini's survey (2018) also showed, in practice, that most of the companies in Europe and the United States were not ready in time for GDPR. Surveys by Dell (2016), KPMG (2017), Addis and Kutar (2018), and Presthus et al. (2018) noted the lack of SA of GDPR to be common in many organisations.

SA was examined widely from other aspects than GDPR. For example, cyber SA was reviewed by Franke and Brynielsson (2014) and Al Sagri and Al Aboodi (2015). E-health privacy risk awareness was surveyed by Bellekens et al. (2016). Pöyhönen et al. (2019) examined cyber SA in critical infrastructure organisations. Argaw et al. (2020) addressed the cybersecurity of hospitals, noting that information sharing simplifies SA and a clear perception of threats and details related to threat actors. Rajamäki and Katos (2020) examined information-sharing models related to cybersecurity early warning arrangements, highlighting the observation that operating protection services as well as for emergency and crisis management were dependent on common cyber SA. They (Rajamäki & Katos, 2019) also observed data analytics techniques (e.g., clustering and classification) promoting SA, when integrated as a part of the information sharing system. Rendall et al. (2021) used a survey to examine cyber threat detection SA. Panagiotis et al. (2019) noticed that Internet of Things (IoT) applications creation requires advanced knowledge extraction and real time situations. Endsley (2000) presented the Situation Awareness Global Assessment Technique (SAGAT) based on the SA requirements of the operator. Sanneman and Shah (2020), in turn, examined the application of SAGAT in measuring the situation awareness of end-users that use autonomous intelligent agents. SA has also been studied from the following perspectives: geo-distributed situation awareness applications in the fog by Saurez et al. (2016), SA related to port security by Adams et al. (2020) in the European Commission's project Scalable multidimensionAl sitUational awaReness sOlution for protectiNg european ports (SAURON), and an intrusion detection system for network security SA by Mahendiran and Appusamy (2018). Vieweg et al. (2014) highlighted that information broadcast through social media may clarify SA during a crisis.

Most recent cyber SA research has been conducted after the research data for this case study was collected in 2021. For example Rowan et al. (2021) leveraged SA approach to examine decision autonomy when individuals concerned the permission for eConsent and Renaud and Ophoff (2021) conducted a SA model to improve the implementation of Cyber security controls and precautions. Ahmad et al. (2021) conducted a model that guides organisations to build a SA of cyber threats and business context emphasising the incident response approach. Insident response side was examined also by Husák et al. (2022). Toxirjonovich and Tulanovna (2022) brought forth the gaps and opportunities related to cyber SA. Technological side approach was represented by Apostolakis et al. (2022) proposed a solution for SA based on Augmented reality (AR) and artificial intelligence (AI), and Chung et al. (2023), Jiang et al. (2002) and DeValk (2022), that examined the visualisation opportunities related to Cyber SA. Schaberreiter et al. (2022) proposed a cybersecurity SA solution for local public administrations referred to developing European legislator cybersecurity framework. They (Schaberreiter et al., 2022) performed the soft systems methodology to support collection, analysis and visualisation processes related to SA process. The comprehensive research (Schaberreiter et al., 2022) is funded by European commission and the research is a part of a project that aimed to create a set of software tools to support the

fight against the use of social media by terrorist organizations and describes for example the layered application architecture for the solution. So after these examples it can be concluded that the mount and types of research of cyber SA has increased in the past few years.

The review produced examples of perspectives on SA from the literature during the last decade. It can be concluded that SA research is diverse and includes both empirical and theoretical research from different fields. However, the previous research does not detail how precisely the SA of GDPR or data DP requirements has been built by the organisations.

3. Methodology

The CS method is used in this article. Bennett (2004) recognised the following aspects as the main advantages of using CS compared to other methods: 1) the notice of new variables and hypotheses and the variables that impact on causal mechanisms, 2) the discovery of history-based explanations for the cases, 3) the increase of the construct validity, and 4) the possibility to use generalisations to model complex relationships. The CS approach was chosen for this study precisely to enable the identification of factors influencing the cause-and-effect relationship related to SA process.

The representatives in charge of GDPR matters in eight either large or medium-sized Finnish organisations with varying industry were interviewed. Interviews were semi-structured thematic interviews and the following 14 open-ended questions presented in table 1 were discussed:

Table 1. **The Interview Questions.**

1. What kind of process was used to build SA of GDPR requirements in the organisation?
2. Who in the organisation builds or utilises SA of GDPR requirements?
3. From which sources outside your organisation have you received useful support for the interpretation or implementation of GDPR?
4. What procedures were used to interpret the theoretical GDPR requirements into practical actions and measures for the organisation?
5. On what basis can the reliability and accuracy of information and data sources related to GDPR requirements be assessed? What kind of information has been relevant and useful?
6. Describe the organisation's experience with GDPR guidance provided by official governing bodies during the process.
7. What kinds of deviations have occurred from the official guidelines during the process?
8. Describe the importance of organisational initiative and activism in the process of building SA of GDPR requirements.
9. How was GDPR-related data management handled in the organisation? What effects has GDPR had on organisational data management?
10. In your opinion, what are the possible causes of occasional inaccuracies or deficiencies in the organisation's SA of GDPR?
11. What has been the most challenging step in building or maintaining SA of GDPR?
12. Are there any differences between building SA of GDPR and other processes in the organisation?
13. What are the most important factors for an organisation to be able to build a correct, comprehensive and reliable SA of GDPR requirements?
14. Describe a successful GDPR-related organisational leadership culture.

4. Results and Analysis

Data was analysed using explanation-building mechanisms, cross-case comparisons, and themes. The kind of set was chosen based on the type of the research question and case types. The results showed that the SA processes for organisations' GDPR requirements varied. Eight types of processes were identified. Typically, the SA process involved becoming familiar with training GDPR content, gathering information within organisations, creating processes, preparing guidelines, training, evaluating, and developing processes and personnel. The processes shared a central focus on the continuous interpretation and integration of data from within the organisation with data from inside and outside of it. Surprisingly, the data coming from inside the organisation became very relevant in the SA process, determining *how* the requirement was implemented in the organisation. The external data, in turn, formed the frames of *what* to do. The core of organisations' efforts during the SA process targeted the organisation internally in implementation awareness and compliance in practice.

According to the responses, the GDPR SA content is typically produced within the organisation at four levels: 1) all staff (day-to-day consideration of GDPR in one's own activities), 2) line organisation level/supervisors (project ownership), 3) DP organisation (GDPR coordination) and 4) executive management (ultimate responsibility, permission and resources for larger projects). The study identified third parties from whom organisations had

received assistance during the GDPR process. It turned out that the understanding of GDPR requirements was influenced by the organisation's own understanding, consultant support, and clarity of authority. It was found that the procedures of organisations to interpret GDPR requirements as concrete actions varied. Assessing the reliability of GDPR requirement information is seen as important, especially for information coming from outside the organisation, as there exists misinformation, misinterpretations, and different levels of service providers (e.g., experienced experts). The information that was the most reliable, but which required interpretation, was considered to be the instructions of the official governing bodies. The attributes of usable control information were defined as follows: unambiguous, filtered, clear, and pragmatic listing that meets customer needs. SA building was also hampered by the following reasons: official guidance information required analysis and was challenging to interpret, not all requests of information are answered, and there are known delays and precedents. Trusted partners were perceived by three interviewees as relevant in the successful interpretation of the requirements. One interviewee also mentioned that more official and more practical control information only became available about 18 months after the end of the transition period (2019–2020), but there was still ambiguity in the guidelines at the end of 2021.

The understanding of what information is in different systems and how it moves was emphasised. The following attributes were referred to as good information management: centralised, in one place, formal, readiness for change, clear communication through different channels, understanding of needs, emphasis on access control, and a system for highlighting important issues (e.g., a ticketing system). The intermittent inaccuracies in SA were mainly due to a lack of understanding of the cross-section of the GDPR in the organisation, shortcomings in formal management communication, lack or inaccuracy in the interpretation of the information collected, and changes and new needs in one's own organisation. Several respondents saw interpreting and coordinating the organisational needs and requirements and business impact assessment (especially new functions) as the most challenging aspects of the SA process.

In the SA process, compared to other processes, the continuous activity and initiative of the organisation was emphasised, as was the fact that it is not a separate but a day-to-day and closely embedded issue for the whole organisation, which requires all staff to understand what is being done. The need for interpretation, ownership, cooperation, support and close business involvement were emphasised. The process of building SA cannot be totally outsourced because outside parties do not know enough about the organisation. The most significant enablers for the success of the SA-building process were identified as the mandate and practical resources provided by executive management (time, people, money), organisational knowledge, careful interpretation of "control data", accountability, commitment, professionalism in GDPR content, training and auditing. Successful leadership required process orientation, clarity (communication, roles, responsibilities, rights), the ability to link requirements to organisational operations and the identification of key personnel, contract management skills, activity, responsibility and overall commitment, as well as strong training for the executive team.

5. Discussion

The model of building optimal situational awareness is proposed here. This threefold model is constructed by combining the findings of an empirical CS analysis, the steps of the intelligence process, and the essential elements of the model of creating information security SA presented by Puhakainen (2016). Generally, the term "intelligence" is used mostly in military science, psychology and technology development and has several definitions. Here the term refers to a process that produces information about an object and circumstances that can then be used to build SA and support decision-making. Puhakainen (2016) examined more than 50 approaches to building information security awareness and, on the basis of his analysis, formulated theory-based IS security awareness (Isec SA strategy). The main elements of the strategy, namely the cognitive and behavioural approaches (Puhakainen, 2016) are used in this model to ensure efficient information security development while building SA of the GDPR requirements. The model is presented in Figure 1 containing the following phases:

1) Data Collection
2) 2-Step Analysis
3) Guidance and Control
4) Distribution
5) Evaluation and Quality

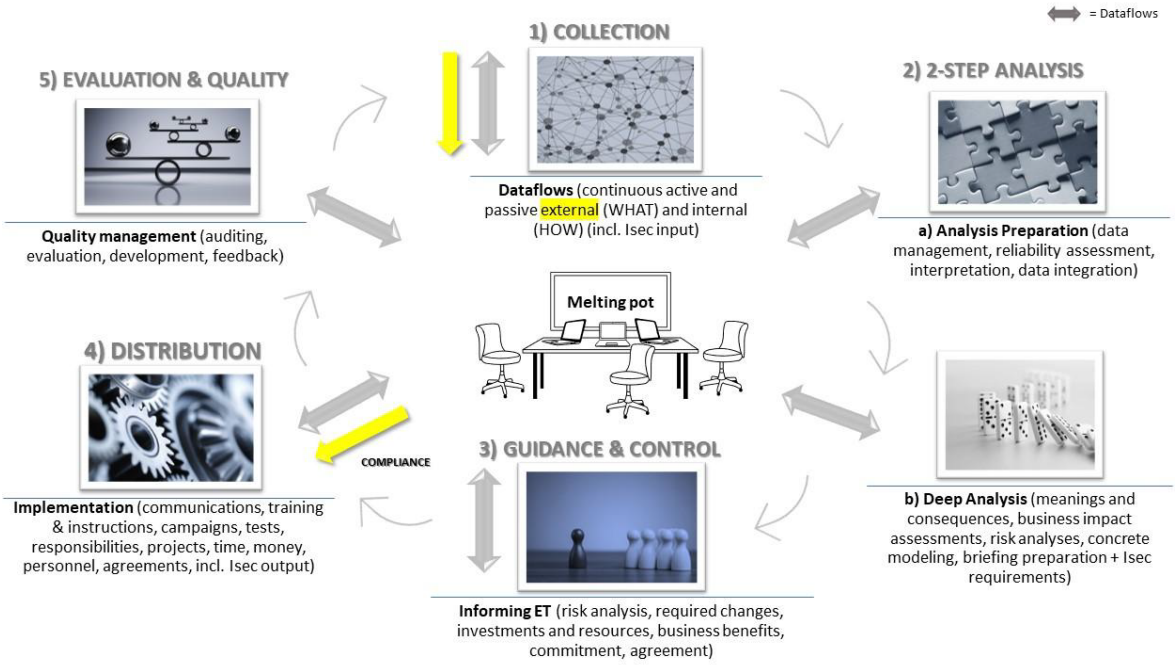

Figure 1. The Model for Building SA of GDPR Requirements.

At the heart of the SA model is the body responsible for building and maintaining SA (DP "Melting Pot"), which actively and continuously collects, processes and shares understanding, gives responsibilities and engages actors in two-way communication. In addition, executive management is kept informed and involved in supporting and enabling the process at all times. Information security demands are involved throughout the process. The following is a step-by-step overview of the model.

Table 2. Description of the Phases of Building SA.

1) Data Collection
Information flows contain information and data from various channels, with differing formats and content. These flows can be actively collected, where the organisation obtains the data through its own activities or, for example, by requesting them from others as a result of collection. These other parties can include industry umbrella organisations, legal partners and so on. Information flows come from outside the organisation (*what* to do) as well as from within *(how* things are done) and identifying the reliability of these flows and their sources is particularly important. External information flows include first-hand sources (EU and national DP authorities), law companies and experts, interbranch organisations, external auditors, ICT service providers, contractors, various training providers, media specialists in DP, external consultants, the partner network, advocacy organisations and peer-to-peer networks. The information flow from within an organisation should be two way: information comes in and enters a process in a fast cycle (e.g., needs, guidance, feedback, questions, requirements, risks). It is important to differentiate, on the one hand, between the layers within the organisation from which different information comes and, on the other hand, those who also need different levels and types of information for their use. Within the organisation, there are five levels, between which the information flows are key: 1) executive management, 2) DP organisation, 3) line management (process and function owners) and 4) all personnel, and the 5) organisation's Isec and Csec functions. If the information flow is not directed from the DP organisation to the organisation at the data collection phase, an information cycle conflict arises, the result of which is that the information flows within the organisation will be incomplete.
2) 2-Step Analysis
Preparatory analysis. At the beginning of the preparatory phase, the key is to ensure the reliability and usability of the data, which means assessing the reliability of the data content and structuring the different forms of data into a specific format to make them usable from both an analytical and a data management perspective. Errors can occur when integrating internal and external data. The data may be corrupt, dirty, old, or misdirected. A properly designed and frequently updated collection plan will partially address these challenges. Errors may also occur in the analysis. The individuals involved in data interpretation and integration are prone to cognitive skew and heuristic distortions. Cognitive skew is a psychological concept, which means that a person tends to perceive and emphasise perceptions, interpretations, and information in certain ways that lead to the wrong result. At worst, cognitive biases can prevent an analyst from perceiving the situation correctly even if all the data and information are in use. Cognitive biases include reinforcement bias, mirror image bias, and vitality bias. In confirmation bias, an individual advocates for information that supports their own preconceptions, gathers evidence, and remembers things selectively. In mirror image illusion, the individual estimates that everyone is acting in the same way as they are. When a situation is hectic, attention is drawn too early and too closely to the "busy" scenario. Heuristics are simplified choice models and shortcuts to thinking requiring as little cognitive effort as possible and are a quick and effortless way to make decisions. A good heuristic is a quick and near-optimal answer, but a bad heuristic, or heuristic distortion, violates logical principles and can lead to wrong conclusions. Heuristic distortions include anchor bias, association bias, and

availability bias. In anchor bias, the wrong initial situation or initial value is taken as the basis for further analysis. In association bias, the transaction is unjustifiably linked to weak or first-come, first-served evidence. In access bias and availability bias, the most readily available data and information are used. Cognitive skew and heuristic distortions in the SA process of GDPR requirements can be prevented and reduced by using the right analytical tools suitable for that analysis. The aim is to remedy these problems by requiring the analyst to be objective in all cases and by training the client to accept or not draw conclusions based on the data generated by the integration. Information must be interpreted in such a way that it is an unambiguous, filtered, clear and pragmatic listing that meets the needs of the user. This includes coordination and impact assessment of the organisation's needs and requirements for the business. It also encompasses Isec requirements as part of other activities, with the assistance of an Isec representative in practical issues (processes, system procurement, upgrades and modifications, training, development, policy, tools, etc.). At the end of the preparation phase, structurally uniform data streams from different sources will be integrated together, including Isec needs.
In-depth analysis. In-depth analysis involves the analysis of combined data, which means interpreting and processing the data into a holistic understanding and evaluating its meanings and impacts. At this stage of the analysis, the interpretation is also based on the assistance of experts. In-depth analysis includes, for example, assessments of the impact and significance of information, risk analyses, selection of priorities, preparation of justifications for development proposals and preparation of these findings for presentation to executive management. Concretised representations of Isec needs will be integrated into the package at this stage.
3) Guidance and control
The findings of the analysis are reported to executive management to make their commitment, support, authorisation and agreement, necessary refinements and practical resources (if needed) available for practical implementation. Also, a plan for integrating the GDPR systematically into business will be made. The necessary changes and additions will be made before final approval and implementation. The commitment of executive management is obtained through training and briefings. Errors related to the distribution of information may include, for example, the analyst modifying the result of the analysis to the liking of a supervisor or other client. Another challenge in distribution is that the customer does not understand or does not want to understand the results of data integration.
4) Distribution
This distribution occurs through communication, creation of guidelines, training, contracts with Isec service providers and other contractors, processes and necessary actions. It is necessary to determine what actions, needs, and responsibilities the implementation includes in practice, what each level of the organisation needs, and what is produced outside the organisation. Staff engagement is implemented through training, division of responsibilities, clear goals, and active two-way communication throughout the process.
5) Evaluation and Quality
Quality management includes, for example, evaluation, development, data management and quality management itself as integral parts of the whole SA process. Emphasis is placed on two-way and active information flows, and in particular on communication within the organisation, observation, feedback and questions, as well as on training and evaluation with the different practices and tools.

Compared to the traditional intelligence process, this model emphasises more open two-way communication as well as commitment and division of responsibilities between different actors, alongside step-by-step analysis before decision-making and guidance. In the case of an organisation's embedded function, the model also emphasises interpretation, ownership, support for collaboration, and the close involvement of the business. The focus of the model is on interpreting and coordinating requirements from within the organisation with respect to external GDPR requirements before making and guiding decisions. During the SA process, the focus inside of the organisation is on implementing practical awareness and compliance while collecting, analysing and reporting information and developing the process. and it is proposed to be leveraged in any abstract issue in a complex environment.

5.1 Implications for Practice

Puhakainen (2016) defined a concept for design theorising regarding Isec SA, which included the appropriate kernel theories, offering instructions for behavioural change, and establishing a testable research approach for scholars. This kind of approach is presented here regarding SA of GDPR requirements. Our article contributes a mixed epistemic–pragmatic model for building SA of any abstract matter in a complex environment. This model enhances the initiation of the necessary actions, reduces the delay in decision-making and embeds the awareness-raising in the organisation's operations holistically. This is realised by, for example, emphasising a more active and integrated relationship between the interpretation and operationalisation of information than what exists in the traditional organisational process. Step-by-step implementation instructions are also described for any organisations that need to build SA of any abstract issue. The model is also a suggested tool for DP, Isec - and Cyber security (Csec) managers that are integrating these security aspects into a single entity. The model is also testable for researchers in future studies. The result is potentially beneficial for building situational understanding of any ambiguous issue, especially in complex and digitalised technological areas, where combining information management with accurate and efficient decision-making is a common challenge.

5.2 Restrictions and Future Study

In this study, data was analysed by using comprising and theming. However, in the comparative study like this, the simultaneous use of the other methods to observe the research problem would have supported more easily to assess the accuracy of the chosen method. Rihoux (2006) analysed the development of the qualitative comparative analysis (QCA), noting that QCA and other related techniques are compatible especially with comparative historical analysis and theory-led case-oriented research. In the future, to support the evaluation of the accuracy of the method could for example these kinds of approaches be considered. One typical limitation of the CS approach relates to a lack of generalisability of the results. The research included experiences from only eight Finnish organisations and there may be differences in experiences in, for example, other EU countries. The larger the samples that are examined and analysed, the more valuable the approaches will be, and overall understanding of the issue will increase. In the future, to fill in the gaps left by limited amounts of empirical research, more empirical evidence of the factors that impact building SA of GDPR requirements is needed. Moreover, more experiences of different SA process building approaches are needed to develop an understanding of the best practices concerning the issue. The model presented here needs to be empirically tested and further experiences are needed to develop it.

6. Conclusions

Previous research has not fully addressed whether organisations have had sufficient SA of GDPR requirements. The aim of this CS was to clarify the landscape of how SA of GDPR requirements is built from an organisational perspective. To guide the CS, we asked how the SA for decision-making was constructed and how it was perceived in eight organisations. The experiences of eight Finnish organisations showed that the organisations' practices of building SA and their experiences with the quality and adequacy of SA differed. Overall, as many different processes were identified as there were respondent organisations. The essential part of the processes included the continuous interpretation and integration of data from within the organisation with data from inside and outside of it. The internal organisational data determined how the requirement was implemented in the organisation and the external data impacted of what to do. The SA process emphasised focusing on the developing organisational implementation awareness and compliance in practice. However, building SA proved to be a critical step for organisations in the overall process of meeting GDPR requirements. Therefore, the main contribution of this research was a mixed epistemic–pragmatic model of building SA. This model, with its detailed implementation instructions, could possibly be of benefit to those building SA of any abstract issue in a complex environment.

References

Aberkane, A. J., Poels, G. and Broucke, S. V. (2021). Exploring Automated GDPR-Compliance in Requirements Engineering: A Systematic Mapping Study. *IEEE Access*, (9), pp. 66542-66559.

Adams. N. P. H., Chisnall, R.J., Pickering, C. and Schauer, S. (2020). How port security has to evolve to address the cyber-physical security threat: lessons from the Sauron project. *Int. J. Transp. Dev. Integr.*, (4:1), pp. 29–41. WIT Press. https://doi.org/10.2495/TDI-V4-N1-29-41

Addis, M.C. and Kutar, M. (2018). The general data protection regulation (GDPR), emerging technologies and UK organisations: awareness, implementation and readiness. *UK Academy for Information Systems Conference*, pp. 1-23.

Ahmad, A., et al. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, 101, 102122.

Al Sagri, H.S. and Al Aboodi, S.S. (2015). Privacy awareness of online social networking in Saudi Arabia. *Cyber Situational Awareness, Data Analytics and Assessment* (CyberSA), *2015 International Conference*, pp. 1–6.

Apostolakis, K. C. et al. (2022). *DARLENE–Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions.* Open Research Europe, 1, 87.

Argaw S.T., Troncoso-Pastoriza, J.R., Lacey, D. et al. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. In *BMC Med Inform Decis Mak* (20), p. 146.

Bellekens, X., Hamilton, A., Seeam, P. et al. (2016). Pervasive ehealth services a security and privacy risk awareness survey. *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA).* IEEE, pp. 1-4.

Bennett, A. (2004). Case study methods: Design, use, and comparative advantages. *Models, numbers, and cases: Methods for studying international relations*, 2(1), pp. 19-55.

Capgemini. (2018). 85% of firms struggle to comply with GDPR by deadline, but opportunity exists for organizations who get it right. *Capgemini's Digital Transformation Institute´s survey: "Seizing the GDPR Advantage: From mandate to high-value opportunity"*. https://www.capgemini.com/no-no/news/85-of-firms-struggle-to-comply-with-gdpr-by-deadline-but-opportunity-exists-for-organizations-who-get-it-right/

Chung, M. H. M. et al. (2023). *Enhancing cybersecurity situation awareness through visualization: A USB data exfiltration case study*. Heliyon, e13025.

Dell. (2016). *GDPR: perceptions and readiness: a global survey of data privacy professionals at companies with European customers*. www.eurocloud.fr/wp-content/uploads/2016/10/gdpr.pdf

Dellinger, A.J. (2019). A Year Later, Many Sites Are Still Failing to Meet Basic GDPR Requirements. https://www.forbes.com/sites/ajdellinger/2019/05/31/a-year-later-many-sites-are-still-failing-to-meet-basic-gdpr-requirements/?sh=5025963d1eb9.

DeValk, K. S. T. (2022). *Real-Time Cybersecurity Situation Awareness through a User-Centered Network Security Visualization*. Doctoral dissertation, University of Maryland, College Park.

Endsley, M. Direct measurement of situation awareness: validity and use of SAGAT. In Endsley, M. R. and Garland D. J (Eds.) (2000) *Situation Awareness Analysis and Measurement*, pp. 147-174. Mahwah, NJ: Lawrence Erlbaum Associates.

Franke, U. and Brynielsson, J. (2014). Cyber situational awareness – a systematic review of the literature. *Computer Security* (46), pp. 18–31. https://doi.org/10.1016/j. cose.2014.06.008.

Hirvonen, P. (2022a). Expectations And Mindsets Related To GDPR. In T. Eze, N. Khan, & C. Onwubiko (Eds.), *ECCWS 2022: Proceedings of the 21st European Conference on Cyber Warfare and Security* (pp. 360-367). Academic Conferences International Ltd. Proceedings of the European conference on cyber warfare and security, 21. https://doi.org/10.34190/eccws.21.1.238

Hirvonen, P. (2022b). A Review of GDPR Impacts on Information Security. *In PACIS 2022: Proceedings of the 26th Pacific Asia Conference on Information Systems. AI-IS-ASIA*: Artificial Intelligence, Information Systems, in Pacific Asia (Article 83). Association for Information Systems. https://aisel.aisnet.org/pacis2022/83/

Husák, M. et al. (2022). CRUSOE: A toolset for cyber situational awareness and decision support in incident handling. *Computers & Security*, 115, 102609.

Jiang, L., et al. (2022). Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access.*

KPMG. (2017). O impacto do regulamento geral de protecc¸a˜o de dados em Portugal. https://assets.kpmg/content/dam/kpmg/pt/pdf/pt-2017-rgpd.pdf.

Mahendiran, A. and Appusamy. R. (2018). An intrusion detection system for network security situational awareness using conditional random fields. *Int. J. Intell. Eng. Syst*., (11:3), pp. 196–204.

Panagiotis, T., Nomikos, N., Michailidi et al. (2019). Hybrid Clouds for Data-Intensive, 5G-Enabled IoT Applications: An Overview, Key Issues and Relevant Architecture. *Sensors* (19:16), p. 3591. https://doi.org/10.3390/s19163591.

Presthus, W., Sørum, H. and Andersen, L.R. (2018). GDPR compliance in Norwegian companies. *Norwegian Conference for IT Use in Organisations* (NOKOBIT), pp. 1-15.

Puhakainen, P. (2006). *A design theory for information security awareness.* University of Oulu.

Pöyhönen, J., Nuojua, V., Lehto, M. and Rajamäki, J. (2019). Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations. *Information & Security: An International Journal* (43:2), pp. 236-256.

Rajamäki, J. and Katos, V. (2020). Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence. *Information & Security: An International Journal* (46:2), pp. 198-214.

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*, 1(1), pp. 24-46.

Rendall, K., Mylonas, A. and Vidalis, S. (2021). Toward situational awareness in threat detection. A survey Edited by: Kim-Kwang Raymond Choo. *Forensic science*. Wires.

Rowan, W., O'Connor, Y., Lynch, L., and Heavin, C. (2021). Comprehension, Perception, and Projection: The Role of Situation Awareness in User Decision Autonomy When Providing eConsent. *Journal of Organizational and End User Computing* (JOEUC), 33(6), pp. 1-31.

Rihoux, B. (2006). Qualitative comparative analysis (QCA) and related systematic comparative methods: Recent advances and remaining challenges for social science research. *International sociology*, 21(5), pp. 679-706.

Sanneman, L. and Shah, J.A. (2020). A Situation Awareness-Based Framework for Design and Evaluation of Explainable AI. In: Calvaresi, D., Najjar, A., Winikoff, M., Främling, K. (eds) *Explainable, Transparent Autonomous Agents and Multi-Agent Systems*. EXTRAAMAS 2020. Lecture Notes in Computer Science (12175). Springer, Cham. https://doi.org/10.1007/978-3-030-51924-7_6.

Saurez, E., Hong, K., Lillethum, D., Ramachandran, U., Ottenwälder, B. (2016). Incremental deployment and migration of geo-distributed situation awareness applications in the fog. *Proceedings of the 10th ACM International Conference*, Irvine, CA, USA, pp. 258–269.

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

Schaberreiter, T. et al. (2022). A cybersecurity situational awareness and information-sharing solution for local public administrations based on advanced big data analysis: the CS-AWARE project. *In Challenges in Cybersecurity and Privacy-the European Research Landscape*, pp. 149-180. River Publishers.

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).* DOI 10.1145/3267357.3267368.

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

Teixeira, G., Mira da Silva, M. and Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, (21:4), pp. 402-418. https://doi-org.ezproxy.jyu.fi/10.1108/DPRG-01-2019-0007

Tikanmäki, I., and Ruoslahti, H. (2019). How Are Situation Picture, Situation Awareness, and Situation Understanding Discussed in Recent Scholarly Literature? In J. Bernardino, A. Salgado, & J. Filipe (Eds.), IC3K 2019 / KMIS 2019: *Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, (3), pp. 419-426. SCITEPRESS Science and Technology Publications. https://doi.org/10.5220/0008494104190426.

Toxirjonovich, O. N., and Tulanovna, X. G. (2022). Situational awareness gaps and opportunities for cyber security. *ACADEMICIA: An International Multidisciplinary Research Journal,* 12(1), pp. 512-518.

Vieweg, S., Castillo, C. and Imran, M. (2014). Integrating social media communications into the rapid assessment of sudden onset disasters. *Social Informatics*, pp. 444–461. Springer: Berlin, Germany.