Studying Data Privacy Management in Small and Medium-Sized IT Companies

Marko Jäntti
School of Computing
University of Eastern Finland
P.O.B 1627, Kuopio, Finland
Email: marko.jantti@uef.fi

***Abstract*—Today, poorly implemented information security and data privacy measures may cause significant threats to companies' existence and business continuity. Additionally, European Union has established strong data protection regulation rules for companies operating within EU. In order to be compliant with these new rules and regulations, organizations have to put a lot of resources to create data privacy policies and plans as well as to adjust tools to manage data privacy requests and fullfill privacy by design and privacy by default principles. Especially for small and medium-sized (SME) Information Technology (IT) firms and software development organizations with limited resources, new GDPR legislation and stricter requirements for information security have caused several challenges and uncertainty on what is adequate level of data privacy. In this paper, we focus on exploring Finnish IT SMEs and their actions and feelings on data privacy and information security. The research problem of this study is: How small and medium sized companies have prepared for growing data privacy and information security requirements? The main contribution of this paper is to show how small and medium sized IT companies in Northern Savo region did prepare for EU data privacy regulation and what types of challenges did exist in the GDPR preparation phase.**

Keywords*—Data privacy; information security; information technology.

I. Introduction

Digital transformation has resulted in new types of security challenges for Information Technology (IT) business and IT departments. Usage of cloud services and cloud-based business systems has exploded due to COVID-19 and software engineering teams have difficulties in aligning IT services with changing business needs and more demanding customer expectations. Additionally, rapidly increasing number of connected systems and Internet of Things (IoT) devices increase vulnerable areas while security attacks are becoming more and more sophisticated and more difficult to detect by traditional security solutions and controls. The role of data privacy became a crucial part of Information System Security and IT service management when European Union initiated General Data Protection Regulation (GDPR) act. During COVID-19 crisis, new type of security breaches have emerged such as forcing video communication system users automatically join some meetings with camera on or trolling video broadcasts with disturbing content.

According to our observations, there are four key data privacy-related challenges that software engineers should also be aware of. The first challenge addresses the commitment of top management in data privacy programmes and projects. Information security and data privacy management should start from top management and should be built in into all company's business activities. Unfortunately often, these are carried out within a small team, typically IT specialists and software engineers and considered as a low priority task among business managers. This may lead to serious problems, if security and privacy are not addressed during service design and implementation. Typically, health care organizations have had more systematic privacy management than organizations from other domains because they had to deal with the privacy concerns long before GDPR regulations to comply with healthcare regulations. Thus, many of the existing GDPR studies focus on healthcare clinics [1]. However, there are still many companies and managers that do not understand the impacts of GDPR to their business adequately.

For example, IT service sales staff might notice that it is difficult to sell GDPR-non compliant services to customers or an organization migh lose valuable points in a tender process due to missing GDPR policies. Additionally, top management should define who is responsible for data privacy internally. In large organizations, establishing a data privacy office (organizational function) with several data protection specialists would be recommendable approach because relying on only one key person (data protection officer) generates a risk. While most of Finnish IT organizations tend to be small and medium-sized (SME) organizations, they typically have one key person responsible for running day-to-day data privacy.

The second challenge is related to managing and storing personal data in cloud services. Rousseaux and Saurel [2] deal with the concepts of safe harbor and privacy shield in the context of big data mining. The concept of privacy shield refers to a data privacy framework between USA and European Union. US-based companies can show that they are committed to comply with the Privacy Shield Framework's requirements. European companies can transfer their personal data to a listed privacy shield compliant service provider without worrying about data processing risks [3]. In order to get a Privacy Shield certificate, an organization should conduct a self-certification to the Department of Commerce in USA [4]. The main idea of Privacy Shield is important to understand from a software engineering viewpoint because growing number of SMEs are using cloud platforms, cloud services or web hosting that are located in US data centers.

The third challenge emphasizes underestimation of GDPR's effects on the whole organization. GDPR affects service design (user interfaces, business logic of intelligent

978-1-7281-8184-4/20/$31.00 ©2020 IEEE

systems [5]), service operation (introducing new privacy-related service request types) and development of software and systems (advanced management of user roles and their rights) in various ways and privacy should be taken into account in systems design from the very beginning [6]. Concerning service design, GDPR introduced a privacy by design principle addressing that organizations should address data protection when they design new services, applications and systems processing personal data. Regarding service operation, companies need to train their staff to understand the basic requirements of data privacy and prepare their front line employees to identify and capture service requests related to data privacy and escalate them to DPOs or data privacy teams.

The fourth challenge is related to understanding and interpreting GDPR policies and principles that are typically written as authoritative legal text. Ayala-Rivera and Pasquale [7] state that it is difficult for practitioners to extract and operationalize legal requirements from GDPR. External consultants are often needed to translate these legal texts such as articles from the data protection directive of European Union [8] into understandable requirements, action plans and data privacy improvement initiatives that are processed through organizational procedures, for example, change management. Martin and Kung [9] recommend that privacy engineering should be introduced and embedded into daily work of software engineers such as risk management, requirements engineering, model-driven design, and software/systems assurance.

Typically, IT service providers need to demonstrate for their stakeholders how they manage information security. This requirement is now extended to include data privacy management and how to proceed in case of personal data breaches. Poorly implemented security and privacy may cause data leaks and damages to brand image and reputation of companies. Service providers should also ensure that all their suppliers comply with required information security requirements. This can be partly achieved by auditing how suppliers comply with basic set of security requirements in international standards such as ISO/IEC 27001 [10], COBIT [11], or ISO/IEC 20000 Part 1: Service management system requirements [12].

Additionally, ISO/IEC 27701:19 [13] is a recent extension to ISO/IEC 27001 and ISO/IEC 27002 standards providing guidance for establishing a privacy information management system (PIMS). Despite all security- and GDPR-related programmes and measures, information security incidents and data breaches may still occur. Organizations should practice the activities how they report on data breaches to national data privacy officers and affected users and customers.

Research gap: Existing academic studies have not adequately studied data privacy management in small and medium sized companies (SMEs). In this paper, we aim at studying data privacy and information security in the context of Finnish small and medium sized companies located in Northern Savo. This regional context is important to note because it affects availability of GDPR consultants and training possibilities. The data for the study was collected during a regional development project.

The main contribution of this study is to show small and medium sized companies prepared for EU data privacy regulation and what types of challenges did exist in the preparation phase. We expect that many of these challenges are still valid and actual to solve. Furthermore, we shall discuss how data privacy was approached by a small service company located in Northern Savo region and what type of decisions they made during their GDPR preparation project.

The results of this study might be useful for information security programme managers, data privacy managers, software engineers, information security specialists, privacy oriented managers and information systems specialists especially in the SME context. The remainder of the paper is organized as follows. In Section 2, the research methods of this study are described. In Section 3, we show the research results including GDPR preparation actions, privacy challenges and changes the GDPR projects resulted in. Section 4 includes the analysis of results. Section 5 presents conclusions.

II. Research Problem & Methodology

The research problem of this study is: How small and medium sized companies have prepared for growing data privacy and information security requirements?

- How SMEs have prepared for data privacy and GDPR regulations?
- What types of challenges are related to ensuring data privacy?
- How SMEs manage GDPR implementation as a change?

These questions are important to answer although the GDPR regulation has been effective since May 2018 in the countries of European Union. There are still many small companies that are not enough aware of privacy requirements and have not implemented required data privacy measures, controls or procedures. Reading the answers of these questions gives SMEs a quick overview how other companies have prepared for fulfilling the requirements of data privacy regulation.

A. Data Collection Methods

Our findings and data were collected during a regional development project by Digital Innovation Hub employee (main author) from multiple companies mainly by interviews, and participative observation in project activities such as a data privacy course. In order to answer this research question, twenty people from service organizations in Northern Savo, Finland were interviewed. The interviews focused on digital transformation and one of the questions in interview questionnaire dealt with preparation for GDPR. Interviewees represented various roles of service organizations such as CEOs, system specialists, business development managers. While some of our case companies are very small entities (VSE), we do not link the role of respondents or any company details to narratives to maintain anonymity of persons. Additionally, we collected information from case Alfa in a separate interview regarding the third research question. In Finland, ethics approval is typically needed in studies related to healthcare or medical research but not in ICT research unless interviewees are children.

B. Data Analysis

Both within case analysis technique and case comparison technique [14] were used to analyze case study data. Tabularization and categorization of case study data were used as analysis techniques. Narratives concerning preparations for GDPR (from interview data) were analyzed by the second author of this paper and translated in English from Finnish. Each narrative resulted in 1-3 categories based on its content.

III. Results

The results of this study were grouped by three research questions: 1. How SMEs have prepared for data privacy and GDPR regulations? 2. What types of challenges are related to ensuring data privacy? 3. How SMEs manage GDPR implementation as a change? These three questions are answerred in the following subsections.

A. How SMEs have prepared for data privacy and GDPR regulations?

The following results were captured from interviews with service organizations. The GDPR question was number 23 in the interview question form (being one of the last questions). However, it provided fruitful answers on GDPR preparation actions. Data was collected by interviewing industry partners of project in 2018-2020. Sample consists of answers (A1-13) from 13 interviewees.

A1: We have evaluated our company's information security and checked which data registers we have. We have studied the principles for storing information, for example, removal times for photos and personal information as well as analyzed what does this mean for our suppliers. We have also participated in GDPR training and obtained a data privacy model (thinking on which level it should be implemented) **Categories:** Information storing, data removal rules, suppliers, training, identification of data registers, information security

A2: We have outsourced the maintenance of the personal data register. **Categories:** Outsourcing

A3: We have created a description how data is processed in our organization. We have participated in GDPR training and prepared a Data Balance Sheet. We have also implemented concrete measures to comply with GDPR such as data processing contracts and identified how our suppliers comply with GDPR. Additionally, we have analyzed our data registers (where personal information exist and what is the information security level of those registers). **Categories:** Data Balance Sheet, training, data processing contract, suppliers, identification of data registers

A4: GDPR was identified on early stage and we prepared for it. When the regulation came into effect, our things were well prepared. I am scared to think how (badly) other organizations have implemented it. We had resources for it. **Categories:** Proactive preparation.

A5: We created required GDPR documents and on technical side we checked and analyzed technical requirements for data logging (users can be fully removed from our system). This is on development stage and almost ready. **Categories:** Analysis of technical requirements, GDPR documentation.

A6: We participated on GDPR training events and were prepared on all areas for GDPR regulations. **Categories:** Training

A7: First, there was a lot of hassle and now nobody talks about it. We have received GDPR training and we appointed a Data Protection Officer. We also limited the access to our customer register, thus only restricted set of people have access to it now. Additionally, we did collaboration with external organization (our IT provider). **Categories:** Training, appointing DPO, consultancy from an external specialist, limiting access to data.

A8: Yes, we have an Information Security team that was responsible for GDPR and we also have provided statements concerning our customers' information systems. I would have needed more information and I think the work is still on progress. I would like to know where I store meeting memos containing personal information. I believe that Information Security team has prepared everything that is needed. **Categories:** Security Team responsible for GDPR.

A9: We could have prepared better for GDPR. On mental level, we have prepared well. We need to apply common sense in adopting it. **Categories:** Common sense in adopting GDPR **A10:** I changed my job and heard that we have GDPR project running here. We have implemented actions related to it and clarified issues in the introduction of a new system. **Categories:** Data privacy clarified in system.

A11: We have been ready beforehand and GDPR issues have been in our control for example how right to be forgotten can work in patient information systems. Our information security team has prepared things. We have started to monitor issues from old insecure applications. Checking 1300 systems is quite a challenge. **Categories:** Proactive preparation, application monitoring, Security Team responsible for GDPR, right to be forgotten, health care perspective. **A12:** We made an investigation what does it mean for us. We organized internal training and analyzed GDPR from the perspective of marketing, what can be done and what is forbidden. **Categories:** GDPR from a marketing perspective, training **A13:** Our service management system is a flexible system and supports well GDPR requirements such as requesting a consent and right to be forgotten. Yes, we have prepared for GDPR. **Categories:** consent management, right to be forgotten.

B. What types of challenges are related to ensuring data privacy?

Concerning challenges organizations faced while preparing for data privacy regulation we found following challenges based on interview data and GDPR workshop discussions:

- GDPR teams should invest more in communication and informing business users (More information needed on GDPR guidelines). Data source: Interview
- Careful preparation and more resources for preparation, especially in SMEs (We could have prepared better for GDPR). Data source: Interview
- Large number of information systems that need to be checked from GDPR perspective (Checking 1300 systems is quite a challenge). Data source: Interview

- Risk management and elimination (in order to manage risks, we identified and removed wrong ways or vulnerable ways to operate business such as removing our e-newsletter) Data source: GDPR workshop
- How to keep users to take care of information security (User is the biggest information security risk) Data source: GDPR workshop
- Organizing job introduction and GDPR training during busy business days (we have many offices around Finland, how to train all the employees systemically) Data source: GDPR workshop

C. How SMEs manage GDPR implementation as a change?

Data for answering the third research question was captured from a case organization Alfa that provides services in Finland and has a very small internal ICT unit that is responsible for maintenance and improvement of information systems. The data was received from discussions with a company representative working in a designer role as well as GDPR-related presentation (1 hour) conducted by the designer. The context of the case is presented in Figure 1.

GDPR implementation was carried out mainly with a company's own resources using a common sense approach and avoiding consultant jargon as well as avoiding purchase of commercial privacy management frameworks and using instead of non commercial privacy guidelines such as VAHTI, the Government Information Security Management Board and Office of Data Protection (Finnish Government). According to the case organization's representative, they had jumped into practical data privacy improvement work without an extensive initial mapping phase. Practical mindset and approach was applied in every stage of improvement. Regarding data privacy risks, certain vulnerable work steps in service operation were removed in order to reduce risks and potential negative consequences. Additionally, we observed that the case organization had established a strategy and vision for their data privacy programme by creating Data Privacy Roadmap.

IV. Analysis

This case study is part of the results of regional development project funded by European Regional Development Fund. One of the project focus areas is cybersecurity involving also information security and data privacy management. Thus, the goal of the analysis was to provide an overview of the GDPR issues from companies' perspective.

As part of data analysis, we first identified a set of categories from the narratives that were obtained from interviews with service organizations participating in regional development project. These categories were later grouped into four main levels (see Table I): Perspectives, GDPR terms, actions, and roles.

Perspectives addressed answers related to viewpoints or domains how GDPR was approached in the organization. GDPR terms addressed the terminology of GDPR concepts found in answers. Actions highlight practical actions organizations took while implementing or preparing for GDPR. Roles refer to roles that were created or utilized during GDPR projects.

TABLE I. How SMEs perform data privacy management?

Area	Categories
Perspectives	Proactive preparation
Perspectives	Health care perspective
Perspectives	Common sense in adopting GDPR
Perspectives	GDPR from a marketing perspective
Perspectives	GDPR from suppliers' perspective
GDPR terms	Right to be forgotten
GDPR terms	Consent management
GDPR terms	Information storing, data register
GDPR terms	Data removal rules
GDPR terms	Data Balance Sheet
GDPR terms	Data processing contract
Actions	Limiting access to data
Actions	Evaluation of information security
Actions	Participation in GDPR training
Actions	Application monitoring
Actions	Data privacy clarified in system introduction
Actions	Consultancy from external specialists
Actions	Analysis of technical reqs
Actions	Creating GDPR docs
Roles	Security Team responsible for GDPR
Roles	Appointing a DPO

Based on our observations in two GDPR training events, many Finnish SMEs are still taking their first steps in GDPR although the GDPR came into effect in May 2018.Some of the interviewees mentioned challenges in aggregating data from multiple sources. In the study of Listokin [15], self-regulation of consumer data and effects of aggregated data were discussed. Aggregated data is information that is collected from multiple sources or with multiple measures, variables, or individuals. Aggregated data is further compiled into data summaries or summary reports. According to the GDPR regulation, the statistical purpose of personal data means that the result of processing data for statistical purposes is not personal data but aggregate data.

Many of the GDPR course participants and interviewees addressed the important role of communication and training in GDPR programmes. Unfortunately often, information security and data privacy remain unclear or even invisible for companies' employees.

Both interviews and GDPR course discussions emphasized the role of external consultants and trainers during GDPR preparations. One interviewee called for common sense in delivering message to staff instead of using consultant GDPR jargon. Some dicussions during GDPR course revealed that many consultants had started marketing GDPR services by highlighting financial sanctions that the organization might receive if they don't start implementing GDPR. During GDPR course discussions, this was generally considered a wrong way to start a GDPR programme. In many cases, GDPR training made by an external consultant had been only opportunity to receive more information what they should do in relation to GDPR. Some interviewees had participated in several different GDPR training (organized by law firms and technical consultants).

Typically, GDPR issues in companies are promoted by Data Protection Officers. Other roles that should receive data privacy training are front-line employees such as service desk staff. None of the interviewees mentioned privacy information management system (PIMS) and logical reason is that it is very young concept. Employees should be trained to identify and capture data privacy related service requests during service

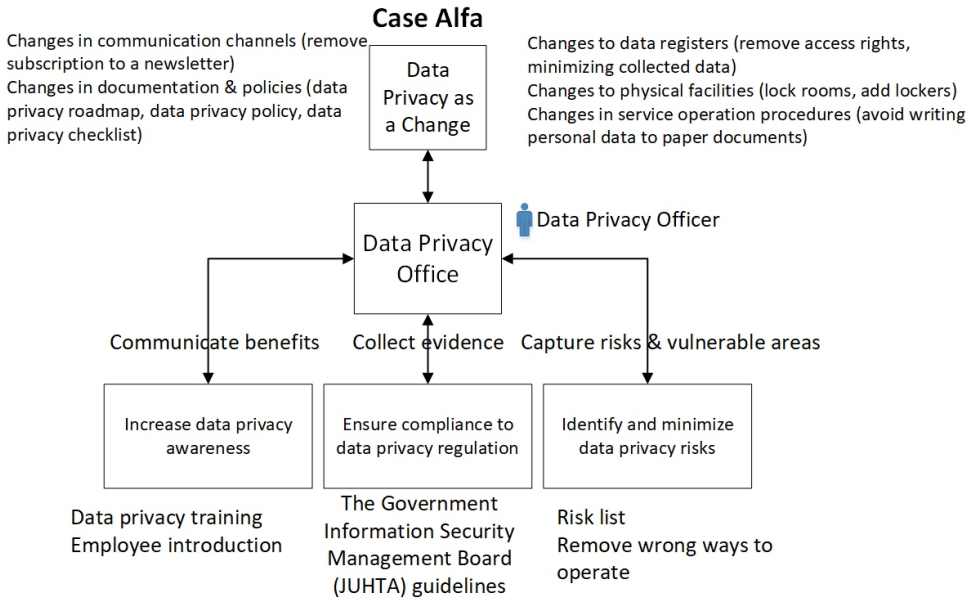

Fig. 1. Research question 3: GDPR implementation as a change

phone calls. The following types of service requests for data privacy and GDPR might be recorded in service desk:

- Request for removing personal data (right to be forgotten)
- Request for restriction of processing personal information (right to restriction of processing)
- Request for transmitting personal data (right to data portability)
- Request for object to processing personal data (right to object)
- Request for not being subject to automated individual decision-making (Automated individual decision-making, including profiling)

Customer self-service portals [16] could have these service requests under service category Data Privacy. Implementing GDPR request management to self-service portals provides at least two benefits. First, privacy requests can be automatically routed to GDPR teams reducing email-based communication and decreasing potential delay in responding or resolving these cases. Second, users or customers can be guided to provide all required data content (mandatory fields) to support their requests which eliminates the need to request missing data from customers. Additionally, data privacy may provide an additional career or specialization area for junior service desk workers [17].

To increase the visibility of data privacy during service design phase, a concept of PrivacyOps could be helpful. In order to understand how PrivacyOps works, it is important to understand the underlying concept of ChatOps that VeriSM framework introduced. VeriSM was designed to cater service management needs on digital age [18]. Basically, ChatOps is a communication approach that supports collaboration and helps teams work together in a virtual chat room. ChatOps aims at supporting conversation-driven development delivery and support. The same chat room can be used to data privacy purposes berween development and operations teams.

By tailoring the ChatOps concept to cater data privacy needs, PrivacyOps provides a place to share, retrieve or display data privacy and GDPR-related information as well as supports training and communication with other team members and even possibilities to automate development and deployment tasks and manage privacy with dedicated tools (manage consents from customers and users) and privacy management processes. PrivacyOps provides a digital bridge between development and operations in all privacy issues and decreases email-based communication and time-consuming meetings. The principles of ChatOps could be implemented with any digital collaboration platform such as Microsoft Teams to manage privacy-related social conversations and information sharing developers and operational teams and could help making these issues more visible in everyday office work.

A single point of data privacy could also help new employees to get a rapid overview which privacy procedures (such as cloud-based file storage) are related to their work and how they affect the daily service operations (for example, event organizers should inform event participants how event registration data is processed and stored). Additionally, discussions during our GDPR training course revealed that many SMEs and entrepreneurs consider it challenging to get a manageable big picture of data privacy. If managers do not have a clear view of what should be done to ensure GDPR compliance, it is not surprise that they also fail in communicating the data privacy strategy and required actions for their employees. More academic studies are needed to study this. In case Alfa, data privacy programme was created and they used a concept of Data Privacy Roadmap to show the direction to their employees.

V. Conclusions

This study aimed at answering the research problem: How small and medium sized companies have prepared for growing data privacy and information security requirements? The research problem was divided into three key research questions:

- How SMEs have prepared for data privacy and GDPR regulations?
- What types of challenges are related to ensuring data privacy?
- How SMEs manage GDPR implementation as a change?

Regarding first research question, the SMEs of our study had prepared for data privacy and GDPR regulations by various ways such as identifying data registers, outsourcing the maintenance of data registers, better monitoring of applications, participating in GDPR training events, creating data balance sheets, reviewing contracts with suppliers, and analyzing GDPR from the business perspective.

Concerning second research question (What types of challenges are related to ensuring data privacy?), the key challenges related to ensuring data privacy included delivering enough data privacy related information and communicating with business users, reserving resources for GDPR preparation, large number of information systems that need to be checked in relation to GDPR compliance. Software engineers and IT specialists should aim at more holistic understanding of data privacy to better understand privacy concerns of business units.

Related to the third research question (How SMEs manage GDPR implementation as a change?), we observed that our case organization had utilize their own resources to prepare for GDPR and relied the GDPR guidelines available through national authorities such as VAHTI the Government Information Security Management Board and Office of Data Protection (Finnish Government). In order to reduce data privacy risks, they had changed some traditional ways to work (reduce writing credit card related information and personal information to paper documents, limit employees' access to personal data). Data privacy roadmap had been introduced to bind various data privacy related improvements, initiatives and separate projects under one programme.

There are certain limitations related to the case study method: First, this study was performed with Finnish service companies in Northern Savo region. The results from other European countries and comparison between our findings and their findings might provide interesting findings for privacy engineering while there can be various differences between EU countries how GDPR is approached. Second, most of our companies providing data for this study were micro, small or medium sized companies. While SMEs have limited resources (rarely have their own legal departments), their approach is more 'adopt common sense and prioritize' than 'prepare for everything' or 'achieve high data privacy maturity' of large companies. Third, our case study did not focus (was not possible) on receiving a deep and thorough understanding on case Alfa but having it as a representative case [19] of a non-ict company that had proactively prepared for GDPR.

Future studies could focus more on studying data privacy of cloud applications and how data privacy is approached by cloud engineers and cloud development teams.

Acknowledgment

We would like to thank the case organization's representatives for valuable inputs and interviews that helped us to perform this study. This paper is based on research in Digiteknologian TKI-ympäristö A74338 (ERDF, Regional Council of Pohjois-Savo).

References

[1] I. M. Lopes and P. Oliveira, "Implementation of the general data protection regulation: A survey in health clinics," in *Proceedings of the 13th Iberian Conference on Information Systems and Technologies (CISTI)*. Caceres, Spain: IEEE, June 2018, pp. 1–6.

[2] F. Rousseaux and P. Saurel, "The legal debate about personal data privacy at a time of big data mining and searching," in *2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)*, Oct 2016, pp. 354–357.

[3] European Commission, "Eu-us privacy shield," https://ec.europa.eu/.

[4] Privacy Shield Framework, "Privacy shield overview," https://www.privacyshield.gov/.

[5] K. Crockett, S. Goltz, and M. Garratt, "Gdpr impact on computational intelligence research," in *2018 International Joint Conference on Neural Networks (IJCNN)*, 2018, pp. 1–7.

[6] F. Blix, S. Elshekeil, and S. Laoyookhong, "Data protection by design in systems development: From legal requirements to technical solutions," in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec 2017, pp. 98–103.

[7] V. Ayala-Rivera and L. Pasquale, "The grace period has ended: An approach to operationalize gdpr requirements," in *2018 IEEE 26th International Requirements Engineering Conference (RE)*, Aug 2018, pp. 136–146.

[8] "Data protection in the eu," https://ec.europa.eu/, accessed: 2018-11-18.

[9] Y.-S. Martin and A. Kung, "Methods and tools for gdpr compliance through privacy and data protection engineering," in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, April 2018, pp. 108–111.

[10] SFS-EN ISO/IEC 27001:2017, *Information Technology. Security techniques. Information security management systems. Requirements*. Finnish Standards Association, 2017.

[11] COBIT 5, *Control Objectives for Information and related Technology: COBIT 5: Enabling Processes*. ISACA, 2012.

[12] ISO/IEC 20000:1, *Part 1: Service management system requirements*. ISO/IEC JTC 1 Secretariat, 2010.

[13] SFS-ISO/IEC 27701:2019:en, *Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines*. Finnish Standards Association, 2019.

[14] K. Eisenhardt, "Building theories from case study research," *Academy of Management Review*, vol. 14, pp. 532–550, 1989.

[15] S. Listokin, "Does industry self-regulation of consumer data privacy work?" *IEEE Security Privacy*, vol. 15, no. 2, pp. 92–95, March 2017.

[16] M. Jäntti, "Exploring self-service support methods in it service management," in *2013 10th International Conference on Service Systems and Service Management*, July 2013, pp. 179–184.

[17] M. Jäntti and H. Kallinen, "Exploring service desk employees' motivation and rewarding," in *2017 International Conference on Service Systems and Service Management*, June 2017, pp. 1–6.

[18] C. Agutter, R. Steinberg, and R. England, *VeriSM - A service management approach for the digital age*. Van Haren Publishing, 2017.

[19] R. Yin, *Case Study Research: Design and Methods*. Beverly Hills, CA: Sage Publishing, 1994.