TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Maria Schlosser 212916IVSB

Designing a Comprehensive Process Bridging the Gap Between Cybersecurity and Data Privacy

Bachelor's thesis

Supervisor: Kristjan Karmo
Master's Degree

Co-supervisor: Katrin Vernik
Master's Degree

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Maria Schlosser 212619IVSB

Tervikliku küberturvet ja andmekaitset ühendava protsessi disainimine

bakalaureusetöö

Juhendaja: Kristjan Karmo
Magistrikraad
Kaasjuhendaja: Katrin Vernik
Magistrikraad

Tallinn 2024

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Maria Schlosser

13.05.2024

Abstract

With the frequency and cost of data breaches and other data-related incidents increasing, small—and medium-sized enterprises face increased risks due to the insufficient implementation of cybersecurity and data protection processes.

This work will research and address the separation between cybersecurity and data protection processes, the lack of awareness among stakeholders, and regulatory compliance.

Primary research is conducted through expert interviews with cybersecurity and data protection experts from varying-sized organisations across industries to obtain a more subjective and practical overview.

The secondary research encompasses journals and articles regarding different pain points within cybersecurity and data protection processes, a comprehensive overview of data breach statistics globally and in Estonia, and an introduction to relevant European Union legislation.

The practical objective of this thesis is to design a comprehensive business process that considers the deficiencies identified in current processes using the Business Process Model and Notation.

This thesis is written in English and is 39 pages long, including 6 chapters, 5 figures and 4 tables.

List of abbreviations and terms

AKI	Data Protection Inspectorate (Andmekaitse Inspektsioon)
BIA	Business impact assessment
BPMN	Business Process Model and Notation
CIA	Confidentiality, integrity, availability
DPIA	Data protection impact assessment
E-ITS	Estonian Information Security Standard (Eesti Infoturbestandard)
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation
ICT	information and communications technology
ISMS	Information security management system
NATO	North Atlantic Treaty Organisation
NIS	Network and Information Security
OÜ	Private limited company (osaühing)
PII	Personal identifiable information
RIA	State Information System Authority (Riigi Infosüsteemi Amet)
SME	Small-medium enterprise
TIA	Transfer impact assessment
US	United States
USD	United States dollar
XaaS	Anything as a service

Table of Contents

1 Introduction 1
1.1 Problem Statement 1
1.2 Aim of the Thesis 2
2 Methodology 4
2.1 Research method 4
2.2 Interviews 5
2.3 Process Design 6
2.4 Business Process Model and Notation 8
3 Literature Review 9
3.1 Cybersecurity and Data Protection 9
3.1.1 Cybersecurity and trends 9
3.1.2 Data Protection 12
3.1.3 Existing Processes 14
3.2 Data Breaches 17
3.2.1 Overview 17
3.2.2 Estonia 19
3.3 Legal Frameworks 22
3.3.1 Network and Information Security Directive 22
3.3.2 General Data Protection Regulation 23
4 Analysis 25
4.1 Analysis of Interview Data 25
5 Development of Process 28
6 Conclusion 35
References 36
Appendix 1 – Non-exclusive license for reproduction and publication of a graduation thesis 39

List of Tables

Table 1. Questions asked of interviewees divided by their position. 6
Table 2. Classification of an enterprise based on staff headcount [15]. 10
Table 3. Overview of the participants interviewed..... 25
Table 4. Roles and responsibilities within the process. 29

List of Figures

Figure 1. Flowchart of the design of the process 7
Figure 2. The statistics of all registered businesses within Estonia are based on their number of employees (Statistikaamet, 2023). 20
Figure 3. The main process integrating cybersecurity and data protection processes. ... 32
Figure 4. DPIA sub-process 33
Figure 5. BIA sub-process. 34

1 Introduction

Data is and has historically been any business' most important asset, and the increasing use of digital services and platforms generates exponentially more data within a single organisation.

The information collected and processed must be adequately safeguarded, managed, and governed throughout its lifecycle, regardless of whether the entity is in the public or private sector.

The increased number of significant data breaches in the past couple of years, worldwide and domestically, poses a challenge to sufficiently secure information, especially personal data.

Data protection and cybersecurity are concepts subject to various interpretations within differing contexts, depending on one’s knowledge, prior experiences, cultural context, and geographical location. However, the absence of either of these processes can have lasting and devastating consequences on an organisation, private or public, from financial loss to reputational damage.

Nevertheless, currently available cybersecurity frameworks cover data protection, a crucial part of both confidentiality and integrity aspects of cybersecurity, on a very high-level basis, creating a clear divide between the technical cybersecurity processes and the legal data governance [1].

1.1 Problem Statement

The majority of businesses in the European Union, as well as in Estonia, are classified as small- and medium-sized enterprises (SMEs), which encounter unique challenges and threats due to their size and the allocation of funds for cybersecurity.

SMEs have lower security readiness and awareness compared to their larger counterparts, increasing their risk of being targeted or exploited by cybercriminals [2], however, their

involvement in the supply chain as service providers to other organisations can have a widespread impact in case of an incident or a data breach.

Supply chain compromise has surpassed malware-based data breaches as one of the main threat vectors of data-related incidents, with phishing and business email compromises being the most common [3].

Despite constant technological advancements in cybersecurity, threats concerning data remain prominent among other significant threats, with adversaries combining more sophisticated attack vectors to target it [3]. Implementing only technological measures achieves limited cybersecurity readiness; therefore, pertinent management activities and organisational processes should be utilised to support a comprehensive security management system further [4, p. 27].

Additionally, the new Network and Information Security Directive (NIS2) enactment sets forth more stringent baseline cybersecurity measures and focuses on strengthening and standardising cybersecurity resilience across member states. Moreover, it expands the scope of the industries and entities it applies to, most of them being SMEs [5].

The compartmentalisation and limited cooperation of cybersecurity and data protection processes can lead to oversights in security controls and activities necessary for compliance, consequently creating vulnerabilities.

1.2 Aim of the Thesis

This thesis aims to identify, analyse, and evaluate existing business processes across multiple industries within different-sized organisations and, considering the findings, design a process integrating cybersecurity and data protection.

The scope of this thesis focuses on SMEs within Estonia, and how current trends across the cyber threat landscapes can influence them.

Based on existing research in data protection and cybersecurity and perspectives attained through expert interviews, a comprehensive and high-level process that could be implemented independently of the entity's sector, industry, or size will be designed.

Privacy and security built into the workflow of development, customer-facing, and other business processes would facilitate a more comprehensive risk analysis and mitigation activities considering cybersecurity and data protection risks simultaneously. This would create a combined interdisciplinary approach to safeguarding organisational assets and individuals' privacy and efficiently managing the entire information security system.

Furthermore, a comprehensive process that encompasses both cybersecurity and data protection measures could offer enterprises of any size the means to govern their data throughout their lifecycle. Additionally, they could monitor and measure the efficacy of existing controls as the process would allow the supplementary safeguarding of other types of confidential data, e.g., intellectual property, company secrets, merger and/or acquisition plans, etc., at an equal level to personal data.

Considering the requirements and guidelines described in GDPR and NI2 in the process design phase will establish a simplified overview of necessary actions and clearly defined stakeholders. This will make the implementation of such processes less intimidating and overwhelming for smaller companies with fewer employees and financial resources.

2 Methodology

This chapter outlines the methods used for researching and analysing varying sources regarding different aspects of cybersecurity and data protection. Those methods include reviewing existing literature, interviews with industry professionals, process design, and the application of the Business Process Model and Notation (BPMN).

2.1 Research method

This work is solely comprised of qualitative data analysis – the primary research consists of interviews with relevant stakeholders, and the secondary research in the form of a literature review of existing research and legislation.

Data collected is commonly divided into two categories: qualitative and quantitative. Qualitative data can be defined as non-numerical information that enables insight into subjective experiences such as perceptions, opinions, and behaviours. Dissimilar to quantitative data, which can be directly measured and expressed empirically, qualitative data allows the analysis of more nuanced concepts, providing a deeper understanding [6].

Qualitative data collection was chosen over quantitative as it provided insight into the organisational culture, attitudes, and intrinsic motivations of the participating parties and allowed for the identification of existing shortcomings of the processes and opportunities for improvement.

In this thesis, primary research is conducted in the form of expert interviews, to gain a versatile and balanced viewpoint of the interactions between different business processes within various organisations across sectors and industries.

The articles and papers chosen were published within the last 7 years on cybersecurity and data protection to ensure current information and relevant themes in the secondary research.

2.2 Interviews

To obtain a comprehensive understanding of the pre-existing processes and their interactions or lack thereof, and get experts' opinions on improvements, interviews with professionals from comparable roles were conducted.

The participants worked in the following industries in Estonia: public healthcare, city government, information and communication technology (ICT), social services, IT and professional services. In total 7 different people were interviewed, and each was assigned an alias based on the NATO Phonetic Radio Communications Spelling Alphabet.

While selecting the sample population, it was important to include both private and public sector entities to cover a diverse range of institutions which might exhibit differing approaches to security management due to budget allocation or financial constraints.

The participants were fully informed that their answers are used as a part of this thesis in an anonymised form to protect their identities and reduce the likelihood of unintended harm. As cybersecurity and data protection are delicate and polarising topics, publishing their places of work might have influenced the interviewees to present an idealised version of the cybersecurity posture and related processes.

Moreover, anonymisation allowed the participants to express their opinions considering weaknesses and critiques of existing processes, decreasing social desirability bias and providing a more realistic overview. Social desirability bias occurs when participants modify their answers to questions to present themselves or their organisation in this case, in a more favourable or acceptable light [7].

The interviews were conducted face-to-face and used a semi-structured format. This means the participants were given background information and the context of this work and then asked open-ended questions.

The interviews were conducted in Estonian as all the interviewees were Estonian and worked in Estonian organisations, however, the analysis of the topics identified from their answers will be conducted in English (see 4.1).

Table 1 outlines the questions, translated into English, that were asked of each interviewee depending on their position and relevant experience. Two questions were common across all the interviews.

Depending on the participant's answer or train of thought, clarifying or follow-up questions that were not prepared beforehand were prompted, such as "Are the processes in place documented and readily made available for all employees", "Are there processes in place in case of a suspected data leak or security incident, and are employees aware of what the expected course of action is".

Five main questions that were asked of each participant were:

Table 1. Questions asked of interviewees divided by their position.

Cybersecurity Professionals	**Data Protection Experts**
What is your opinion on the current state of cybersecurity landscape in Estonia?	What is your opinion on the current state of data protection landscape in Estonia?
Describe the depth of your knowledge regarding the relevant regulations to ensure sufficient protection of personal data.	Describe the depth of your knowledge regarding technical measures to safeguard confidentiality and integrity of data.
Are there any predefined processes for cybersecurity / security management?	Are there any predefined processes for data protection in your institution?
How do you currently see the cooperation between cybersecurity professionals and data protection experts within an organisation?	
Describe the different ways you'd improve the interoperability or communication between the cybersecurity and data protection processes.	

2.3 Process Design

While planning and designing the process, it was significant to incorporate as many different processes related to cybersecurity and data protection as possible to ensure an interdisciplinary approach that would benefit a wide range of institutions.

Figure 1. Flowchart of the design of the process provides a concise overview of the steps taken to create a process that meets those criteria.

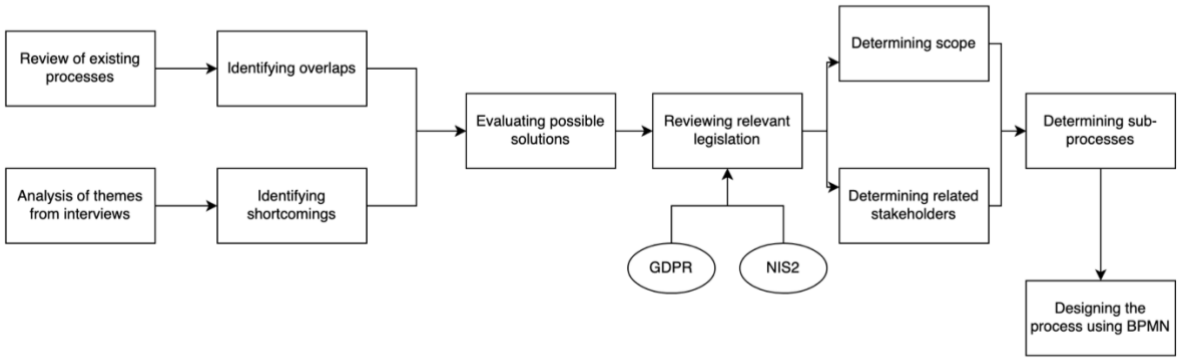

Figure 1. Flowchart of the design of the process

The design of the process involved the analysis of the current and future cyber threat landscape, overlapping aspects of current cybersecurity and data protection processes, and identifying deficiencies revealed by existing research in addition to feedback received from the interviews.

Additionally, it was important to incorporate requirements set forth by GDPR and NIS2 in the process, to ensure compliance, as those two regulations are currently the most influential in the EU.

Once the gaps were identified and the objective of the new process was determined, relevant stakeholders had to be assigned. The minimal possible number of stakeholders was selected to account for SMEs' possible resource constraints while ensuring the process's integrity.

The scope of the process had to be defined as cybersecurity covers a broad range of assets, including physical assets, which have different protection requirements than digital assets. This process will, therefore, only focus on IT business assets.

After the roles and their respective responsibilities were outlined, a rough draft of the process was created to identify any sub-processes that should be included with the main process. After evaluating the data, two sub-processes were decided upon: business impact assessment (BIA) and data protection impact assessment (DPIA).

The final step was to model the process using BPMN, considering all the abovementioned factors.

2.4 Business Process Model and Notation

BPMN or ISO/IEC 19510 is a graphical representation of business processes in a business process model, based on a flowcharting technique, creating a bridge across the gap between process design and implementation [8].

The selection of BPMN for this work was due to its ease of use and straightforward comprehensibility along the entirety of the corporate structure, ranging from business analysts to new hires, and it allows the deployment and monitoring of the processes in a standardised and concise manner [9], [10]. Additionally, BPMN-based process models can be created using a wide variety of software solutions, including but not limited to open-source software like Bonita BPM, freeware options like Bizagi, or proprietary software such as Enterprise Architect, thus making it accessible to small, medium, and large enterprises alike, independent of their financial constraints [10].

Moreover, the handbook published by the Ministry of Economic Affairs and Communications of Estonia, focusing on the business processes of the public sector and their analysis, recommends the use of BPMN for process modelling [11]. This allows an effortless adoption of the processes designed and modelled within this thesis, thereby ensuring ease of implementation.

3 Literature Review

3.1 Cybersecurity and Data Protection

This section will explore the definitions of cybersecurity and data protection, give an overview of some existing research on the topics, and introduce pre-existing processes.

3.1.1 Cybersecurity and trends

A study by Althonayan and Andronache defines cybersecurity as "the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and individuals' assets." [12].

This comprehensive definition is why this work uses the term "cybersecurity" in place of "information security", emphasising a holistic approach to ensure the confidentiality, integrity, and availability of data throughout the entire organisational process structure, including but not limited to employees and third-party service providers.

Furthermore, Estonia's transposition of the EU's Network and Information Security Directive, the Cybersecurity Act, uses the term "cybersecurity" in place of "information security" [13].

The majority of cybercrimes are motivated by either espionage, information theft, or financial gain, with the government, defence, financial, telecommunications, and healthcare being the most targeted sectors. 86% of data breaches have financial motivation behind them, with adversaries selling credentials, personal data, email addresses, etc., on the dark web in exchange for Bitcoin or other cryptocurrencies [14].

Additionally, small and medium-sized enterprises (SMEs) have become valuable targets for cybercriminals regarding threat vectors such as data breaches, data erasure, and denial of access to data due to their lack of expertise, ungoverned outsourcing, and outdated security measures [2], [5].

A company is considered to be an SME based on either its number of employees or its turnover or balance sheet total. In the context of this work, staff headcount will be used

to determine the size of an organisation; the specific ranges have been expressed in Table 2 [15].

Table 2. Classification of an enterprise based on staff headcount [15].

Company category	**Staff headcount**
Medium	< 250
Small	< 50
Micro	< 10

During difficult economic conditions and the increasing popularity and convenience of anything as a service (XaaS), many smaller companies opt for using third-party service providers due to cost restraints, and to keep up with the rapidly changing technology trends and landscape [2], [16].

With the overreliance on anything as a service (XaaS) and the high cost of cybersecurity solutions, critical vulnerabilities present in SMEs' internal infrastructure can have a widespread effect on the supply chain's security as a whole due to poor cybersecurity practices [5].

Moreover, these third-party service providers or vendors are often small- or medium-sized companies themselves with limited financial resources who are focusing on maximizing their profits and reducing costs. This leads them to disregard sufficient cybersecurity measures and increase their overall risk of cyber-attacks [2], [17].

Whilst the use of vendors or XaaS, such as cloud computing, provides small and medium-sized enterprises opportunities for growth and increasing their competitive advantage, Alahmari and Duncan argue that the main risk factor of SMEs is the threat to their cybersecurity stemming from a lack of awareness and underestimating cyber threats [2].

The human component, or system user, is widely accepted and known as the weakest link in the cybersecurity process, therefore it is imperative to excogitate this variable from a multidisciplinary perspective, considering that errors made by expert users involved in critical aspects of the business can have severe or even debilitating consequences [18].

Despite the quantity and/or quality of the technical controls implemented in an organisation's security management process, the dereliction of general awareness and knowledge resulting in the omission of security controls within sub-processes can decrease the entity's cybersecurity resilience and open them to more vulnerabilities.

For instance, Lopez et al. found in their study that software developers do not consistently use best cybersecurity practices and solutions within the development process, considering the security of the code they're writing a secondary matter. Furthermore, they relied on the intrinsic security features in the technologies, depending on pre-existing code, e.g. a built-in permission system [19].

The consistent use of component-based code or open-source libraries to consolidate the development processes, however, could induce unmonitored interactions between applications, thereby creating novel and unexpected vulnerabilities not only within the respective program but also throughout the whole supply chain. Hence, malicious actors can exploit these vulnerabilities to compromise data or systems on both the supplier and customer fronts [16].

Furthermore, the security of the development projects was seen as an external, event-based requirement which produced a predetermined list of "things to fix" within the scope of an audit conducted by a client or partner [19].

This demonstrates that cybersecurity may not be integrated into other sub-processes whilst secure processes are implemented and managed by a security specialist or even top management. Moreover, there may still exist a gap in the understanding of the concept of "secure" across departments and roles, resulting in the insufficient implementation of security controls in the development process. These oversights might remain undiscovered until the application or service has gone live and the vulnerabilities within have been exploited.

These trends outline that data has become a valuable resource among cybercriminals, making investing in cybersecurity and data protection more important than ever.

3.1.2 Data Protection

The concept of data protection can be understood through diverse perspectives, influenced by factors like industry-specific definitions, regulatory and legislative frameworks, and different geographical locations.

For example, the Storage Networking Industry Association defines the principle of data protection as the “deployment of methodologies and technologies to protect and make data available under all circumstances”. It highlights the fact that what is seen as “data protection” in the EU is commonly defined in other regions as data privacy [20].

Any information or business asset that allows the direct identification of a person or allows one to be singled out and identified through further research is classified as personal data and treated in the same manner under the GDPR [21].

Although pseudonymisation can reduce security risks for data subjects and enable statistical business analysis of data, it is not exempt from the GDPR's scope as it is still classified as personal data [21].

Ensuring the privacy of personal data and other business-critical information, including but not limited to proprietary information, process documentation, and intellectual property, can be viewed as a functional outcome of security practices and comprehensive data protection measures. This aligns with the overarching goal of preserving and ensuring business assets' continued availability, confidentiality, and integrity [22].

Moreover, Bertino (2016) argues that in addition to the pre-established criteria of data security: confidentiality, integrity, and availability, privacy should be considered an additional critical requirement in data security and protection. Despite their similar meanings, privacy does not equal confidentiality. Keeping data safe from external threat actors and malicious insiders does not ensure the data is collected, used, and shared in compliance with relevant legislation, such as the GDPR.

The same study discusses the importance of data trustworthiness, ensuring that data stored by an organisation remains impervious to modifications made by unauthorised entities, free of errors, up to date, and originates from trusted sources. This suggests that the aforementioned concept should be incorporated as an aspect of the integrity requirement [23].

This exemplifies that the requirements set forth by the GDPR and other legislation focusing on data privacy can be easily incorporated into the traditional CIA triad of cybersecurity. It also provides additional value to traditional business processes by ensuring accurate and current data is used for analysis and decision-making.

When discussing technical data protection measures employed during the development process, the same risk persists, as mentioned in the cybersecurity chapter (see 3.1.1) regarding the awareness and expertise of software developers.

GDPR Article 25 outlines that "… the (data) controller shall, both at the time of determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures…" However, the regulation provides limited guidance on implementing specific technical or organisational measures, creating ambiguity and allowing affected parties to implement only the minimum controls necessary for compliance [24], [25].

Aljeraisy et al. found that due to the GDPR's ambiguous guidelines and the lack of practical, industry-specific guidance that considers the technical domain to ensure data protection during the development process, data privacy is seen as an extra, sometimes optional step, and the practical necessity of privacy-preserving controls is not understood [24].

Lack of knowledge about data protection requirements can accidentally lead to non-compliance, as technical stakeholders might not be aware of the difference between anonymisation and pseudonymisation, for example. Although pseudonymisation replaces identifiable information, such as names or addresses, with pseudonyms or codes, pseudonymised data is still classified as personal data and is subject to the GDPR [21].

Rather than managing the separate risks arising from developers' lack of knowledge through two disjointed processes and imposing two sets of controls that might have a significant overlap, one stemming from the cybersecurity management process and the other to achieve regulatory compliance, a more efficient approach can be taken. By identifying controls from both processes that, when combined, would provide equivalent safeguards, both data protection and security can be ensured at a sufficient level through an integrated process.

Furthermore, this approach would allow the institution to concurrently manage and monitor the risks outlined, leading to an improved overview of the security management system's effectiveness along with ensuring compliance as the misuse and damage of data can have far-reaching repercussions, affecting not only single individuals or organisations, but also spanning entire social sectors and critical infrastructures, and essential services [23].

An increasing number of EU consumers have begun expressing rising concerns regarding the use of their data online and are seeking not only the ability to access and modify their data but also to gain greater control over access and usage rights additionally [16].

Furthermore, a 2020 study by Romansky et al. found that while 74% of EU citizens perceive personal data as an increasingly integral part of the digital world, merely 26% of social computing users and 18% of online shoppers believed that they possessed full access to their data, emphasising the disparity between the amount of data collected and the existent control they believe they have over the processing and storage of their data.

Despite the increased urgency to protect customers and their data, several institutions can be found lacking as demonstrated by the statistics (see 3.2.1), proving that regardless of the security and data protection measures, organisations can still be harmed through their least secure link, like a third-party service provider. Hence, it should be crucial for all entities that process and store personal data to re-evaluate the amount of data they collect, and limit the extent of storage of unencrypted personal data [17].

3.1.3 Existing Processes

ISO/IEC 27001

One of the most recognised international standards for information security, ISO/IEC 27001, addresses cybersecurity through a risk-based approach, business processes and their interactions.

The standard ensures that secure handling and sufficient protection of information assets are conducted throughout the entire organisation. It states the importance of including all processes throughout the organisation and the overall management structure in the ISMS. Furthermore, it emphasises that information security should be considered and assured in the design of processes, information systems, and controls [26].

Although the 2013 version of ISO/IEC 27002 contained a control aimed at protecting personal data, the 2022 version introduces three new controls that focus on data protection [4].

Control 8.10, information deletion, outlines the need to erase any information that is no longer required to prevent the exposure of sensitive information. Additionally, it provides guidelines on what, when, and by whom the data should be deleted [4].

Control 8.11, data masking, describes different techniques to mask information, such as anonymisation or pseudonymisation of personal data, technical methods, and explains the differences between the two [4].

Control 8.12, data leakage prevention, outlines different measures that can be taken to detect and prevent the disclosure of information, providing methods to reduce the overall risks of both stored data as well as backups [4].

Estonian Information Security Standard

Estonian Information Security Standard or E-ITS is an information security standard that has been developed using BSI IT-Grundschutz, a German standard, as its foundation, and in its development, compliance with ISO/IEC 27001 has been considered [27].

The objective of E-ITS is to provide comprehensive protection of business processes and information systems to achieve a standardised level of security throughout the entire data lifecycle by managing operational risks [27].

E-ITS is considered a baseline security framework as it outlines common risks and vulnerabilities and prescribes controls to mitigate them depending on the institution's protection requirements. However, the standard encourages performing additional risk analysis to ensure that all business assets are sufficiently safeguarded [28].

It is managed and updated annually by the State Information System Authority (RIA) and it is supported nationwide in addition to aligning with relevant Estonian legislation, such as the Cybersecurity Act, which is the transposition of the EU's Network and Information Security Directive (NIS) [13], [27].

CON.2: Protection of personal data is the module that outlines controls for secure data processing which are divided into three distinctive sections: planning (kavandamine), implementation (evitus), and operation (käitus) [29].

Some of the important guidelines given regarding the mapping of protection measures, ensuring the legality, purposefulness, and minimality, and the proper retention of personal data processing [29].

In contrast to ISO/IEC 27001, E-ITS describes the importance of involving data protection officers in the cybersecurity process to ensure compliance with GDPR and assess data processing-related risks. Moreover, it outlines specific Estonian legislations and relevant paragraphs that the organisations are required to comply with, giving a concise and detailed overview [29].

Data Protection Impact Assessment

Unlike the previous cybersecurity processes discussed, the data protection impact assessment (DPIA) is the only process required by EU law if an entity processes personal data.

Article 35 of the GDPR outlines that DPIA should be conducted when the processing activities are likely to result in a high risk to the rights and freedoms of the data subjects, particularly in cases of large-scale evaluation of personal aspects, such as profiling, processing of special categories of personal data, such as genetic data and sexual orientation, or when the data collection occurs during systemic monitoring of a publicly accessible area [25].

Furthermore, DPIA should be conducted in all cases where the data will be transmitted outside the EU; therefore, if organisations use XaaS services that are located outside the EU/EEA, they are legally obligated to perform and maintain a DPIA [25], [30].

In addition to a DPIA, a transfer impact assessment might need to be conducted to ensure sufficient safeguards on the personal data both in transit and at rest, such as cryptographic algorithms, additional access control measures or processing limitations put on the service provider [25].

Four set aspects need to be present in a DPIA, which are:

1. Assessment of whether the processing of personal data is necessary and proportionate.

2. Comprehensive description of the planned processing actions of personal data and the purposes.

3. Assessment of the risks that may threaten the rights and freedoms of data subjects.

4. Intended measured for addressing risks, including requirements, processes, and systems ensuring the protection of personal data and compliance with the GDPR, considering the rights and legitimate interests of data subjects and other relevant parties [25].

Although DPIAs are not mandatory for all processing operations involving personal data, AKI recommends organisations that handle personal data to map out the extent of the processing to understand whether their activities comply with regulatory requirements [30].

Furthermore, incorporating data processing relating risks to any entity's risk management process would provide a comprehensive overview of all information-related risks and related mitigation activities in addition to applying technical controls to further safeguard their information assets.

3.2 Data Breaches

3.2.1 Overview

A data breach can be described as an unauthorised access, disclosure, or procurement of sensitive or confidential information, including but not limited to personal data, leading to its loss, exposure or compromise to unauthorised parties or entities, such as an unauthorised use or theft of business information from the company's network, systems or applications [17], [31].

The IBM Security report outlines that the global average cost of a data breach has reached 4.45 million USD in 2023, when in comparison, it was 3.86 million in 2020, a 15.3% increase. The reported mean time to identify (MTTI) a data breach was 204 days and the

mean time to contain (MTTC) was 73 days in 2023, with the values being similar to previous years' results in both aspects [32].

This illustrates that it takes on average 204 days for a company to determine a security breach has occurred and then an additional 73 days to resolve it once it has been uncovered, giving malicious actors nearly a year undetected within a company's systems and databases.

Moreover, the most prevalent type of data compromised during a data breach was customers' personal identifiable information (PII), or personal data as defined by the GDPR, with 52% of all breaches containing some type of customers' personal data. That was followed by employees' PII with 40%, and then intellectual property with 34% [32].

The 2023 IBM Security report included statistics regarding the proportionality of supply chain attacks and the associated costs, providing insights into software and business partner-related incidents.

15% of institutions outlined business partner supply chain attack as a source of a data breach, i.e., the compromise originated from an attack on their business partner. The financial repercussion of such a compromise was 11.8% higher, and the MTTI was 27 days longer than the average. Additionally, software supply chain attacks accounted for the data breach occurrences in 12% of the institutions, i.e., the threat actor pervades a vendor's network to compromise the software prior to it being sent out to the customers, allowing the infected software to attack the customer's systems. Equivalently to the business partner-related incident, the cost of such an attack was 8.3% higher and the MTTI was 15 days above the average [32].

This exemplifies that in addition to managing the institution's cybersecurity-related risks, it is imperative that additional risks to data security and protection that are posed by using third-party vendors are also managed and mitigated, as incidents through the supply chain can have more severe consequences, in terms of financial losses in addition to response times.

The SolarWinds cyber-attack, carried out by a possibly state-sponsored adversary in 2019 can be used to demonstrate the devastating effects that software supply chain attacks can have not only domestically but on a global scale. Orion, a system distributed by

SolarWinds was compromised by an injection of malicious code within its update package, which was then spread to SolarWinds' clients' networks, creating a backdoor allowing the exfiltration of performance and other data generated by IT assets' logs. Over 18,000 customers were impacted by the infected update, including Fortune 500 companies in addition to multiple US government agencies confirming that even the entities with strong security measures could be exposed to a data breach [33], [34].

This exemplifies the importance of not only managing the cybersecurity risks inherent to the singular institution but furthermore establishing processes to mitigate any additional risks to data security and protection presented by external service providers. Incidents originating from the supply chain can result in more severe consequences, such as financial losses and longer incident response times.

The biggest factors increasing the cost of a data breach were security system complexity, security skills shortages, and non-compliance with regulations. It is noteworthy that only 51% of companies that had experienced a data breach reported that they were planning to allocate additional funding following the incident [32].

Organisations often refrain from notifying their customers or employees that their personal data has been compromised, as they expect potential loss of trust and damage to their reputation, which may deter potential customers. Consequently, the statistics outlined above may not accurately portray the true prevalence of data breach occurrences [35].

3.2.2 Estonia

The data breach and cyber threat landscape in Estonia reflects global trends as outlined in the previous section, indicating an increasing number of data related incidents both globally and domestically.

In 2023, RIA offered grants valued up to 60,000 euros to SMEs to work with a consultant to map and evaluate the security of their systems, products, and services, consequently increasing their overall cybersecurity posture [36].

According to Statistics Estonia, a government agency that is responsible for providing relevant and reliable information and ensuring the quality of data on a national level,

SMEs make up 99.9% of all the companies registered in Estonia with the majority of them having less than 10 employees as illustrated by **Error! Reference source not found.**.

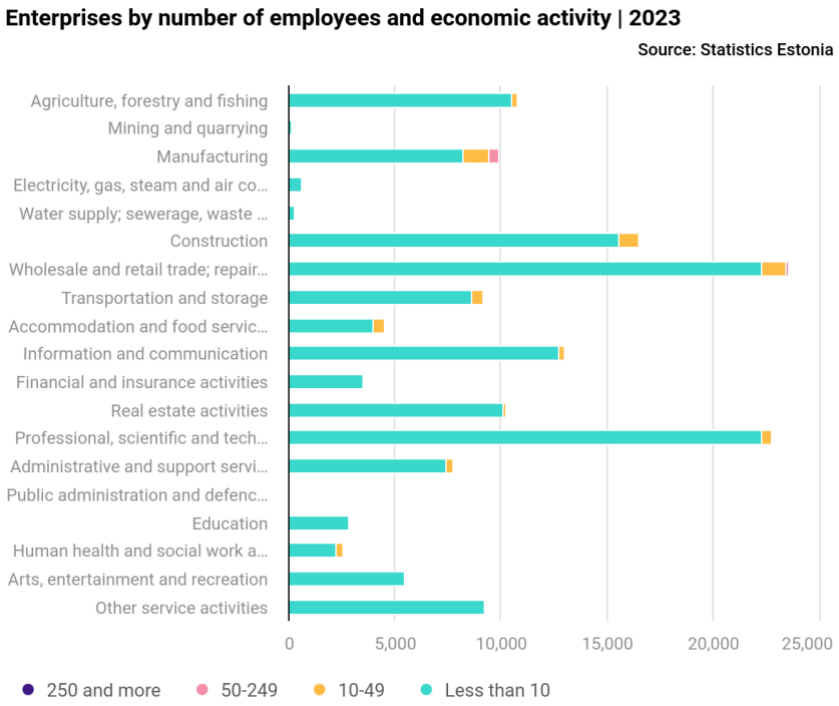

Figure 2. The statistics of all registered businesses within Estonia are based on their number of employees (Statistikaamet, 2023).

According to RIA, SMEs are less prepared to handle cybersecurity-related incidents compared to their larger counterparts. While they are progressively adopting digital solutions to remain competitive, they may overlook the necessity for security measures due to financial constraints [36].

Moreover, RIA emphasises how threat actors can use a service provider's vulnerabilities to therefore compromise or affect their clients' systems, illustrating the widespread consequences of a supply chain attack and how the weaknesses of partners can easily influence others [36].

Consistent with global statistics, the data published by the Data Protection Inspectorate (AKI) supports the upward trend of data-related incidents and infractions.

AKI is an independent supervisory authority under the Ministry of Justice, overseeing and enforcing compliance with personal data protection laws, establishing a fair

counterbalance between individual rights, public interests, and business concerns. Moreover, AKI contributes to the development of relevant legal frameworks, ensuring that violations involving the processing of personal data are stopped and the constitutional rights of Estonian citizens are protected [37].

Analysing publicly available statistics from AKI's website reveals a notable trend: the number of personal data breach notifications surged from 936 in 2022 to 1,068 in 2023, representing a 14.1% increase. Similarly, the count of reported data breaches rose from 153 in 2022 to 196 in 2023, indicating a significant 28.1% increase [38].

Two companies, Asper Biogene OÜ and Allium UPI OÜ, experienced the most significant data breach incidents in the country's history in the span of a year. Both companies are classified as SMEs, with Asper Biogene OÜ employing 13 people and Allium UPI OÜ employing 79 [39], [40].

In November 2023, Asper Biogene reported to the police that they identified an intrusion to their database and various files had been downloaded. The compromise had a span from 2009 to today, with 33 gigabytes of data exfiltrated. Over 100,000 different files were affected by the incident and approximately 10,000 of Asper Biogene's clients' health information was affected [41].

Moreover, since the data breach, it was reported that there had already been an attempt to extort money from an individual who had connections to the data leak. The person was called by the perpetrators and informed that their information was compromised [42].

In February of the following year, 2024, Allium UPI disclosed that the loyalty card system managed by them had been compromised and customers' data, including but not limited to personal ID codes, email and home addresses, and phone numbers stemming from a backup copy of a database. The impact of this attack was unprecedented, affecting 700,000 customers, which accounts for almost half of Estonia's population, demonstrating the scale and extent of the breach. Dissimilar to the Asper Biogene incident, the police investigation cooperation extended beyond Estonia's borders [43].

The heightened susceptibility and distrust resulting from a significant data breach incident, such as referenced here, could therefore contribute to a rise in phishing attacks. This could be associated with the accessibility of personal information and the created

uncertainty within the affected population, creating a suitable psychological context for a successful phishing attack.

3.3 Legal Frameworks

This section describes the two relevant pieces of legislation that organisations are subjected to and their applicability to the processes.

3.3.1 Network and Information Security Directive

The Network and Information Security Directive (NIS2) is EU legislation regarding cybersecurity resilience across the member states that came into effect on January 16, 2023, and it repeals the first NIS Directive. All EU member states are required to transpose it into national legislation by October 2024. In Estonia, the corresponding legal act is called the Cybersecurity Act (Küberturvalisuse seadus) [5], [13].

NIS was originally developed to help increase cybersecurity competencies, mitigate threats, and provide guidelines to ensure the continuity of essential services across the entire European Union. However, considering the progression of the cyber threat landscape and the increased focus and reliance on digital systems in everyday life, the measures outlined in NIS were found to be insufficient and vague [5].

To address and mitigate the identified gaps within NIS, in 2022, NIS2 was introduced which expanded the scope, defining additional services as essential, including more sectors, medium-sized companies, public entities, and digital service providers [5].

NIS2 aims to standardise the level of cyber resilience among the member states by providing more specific security requirements and clearly defining essential and important entities, hence establishing a baseline cybersecurity across the EU [5].

Some of the mandatory measures outlined in NIS2 are policies of risk analysis and management, business continuity, supply chain security, including secure procurement of services, cyber hygiene practices and sufficient cybersecurity training, and the assessment of the effectiveness of risk management controls [5].

Furthermore, the directive states that member states should address the cybersecurity needs of SMEs through their national cybersecurity strategies and support them in the

improvement of their cybersecurity posture as SMEs form a large part of the supply chain [5].

With NIS2 imposing more stringent penalties for non-compliance, the absence or implementation of an ineffective cybersecurity process can result in severe financial repercussions.

Non-compliance with the measures set forth by Articles 21 and 23 may lead to administrative fines of up to 10 million euros or up to 2% of the organisation's yearly turnover if the infringement is committed by an essential entity. Alternatively, fines may amount to up to 7 million euros or up to 1,4% of the total turnover if it's by an important entity [5].

3.3.2 General Data Protection Regulation

The GDPR aims to balance the protection and privacy of individuals and their data, while simultaneously facilitating the justified processing of such data to support social and economic progress [25].

The regulation came into effect on May 25, 2018, as it was found that the technological advancements and the increased scale of collection and processing of personal data introduced new challenges and risks that were not adequately addressed by the previous data protection directive [25].

All processing activities of EU citizens' personal data are protected under the GDPR, regardless of the processor's location, as long as the organisation provides products or services to individuals residing within the EU [25].

Article 5 of the GDPR outlines the seven core principles of data processing: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity; and confidentiality. In essence, these principles describe the actions that data controllers should take to ensure the protection and privacy of personal data [25].

Additionally, the organisations need to implement and be prepared to demonstrate compliance with a separate principle outlined in the same Article, accountability. As a result, institutions with more than 250 employees need to create and manage

documentation on what type of personal data is handled, for what purposes, what are the safeguards put in place, and what processing activities are conducted by a processor [25].

Data processors perform personal data processing activities on behalf of data controllers based on a contractual agreement that outlines the nature of the processing and the controller's obligations and rights [25]. Most business-to-business service providers can be considered data processors.

Although SMEs are exempt from the GDPR’s requirement to document their data protection processes, maintaining and managing current and written evidence of compliance may result in lesser penalties when data-related incidents occur within the organisation.

Similarly to NIS2, if non-compliance is identified, the legal entity may be subjected to administrative fines of up to 10 million euros or up to 2% of their yearly turnover, whichever is larger at the time of proceedings [25].

4 Analysis

This chapter will focus on the in-depth analysis of the data obtained from expert interviews, identifying common themes regarding cybersecurity and data protection processes and relating attitudes.

4.1 Analysis of Interview Data

As discussed further in the Methodology section of this thesis, the participants were chosen based on their positions and the industries they worked in to provide a broad overview of the existing processes implemented across different sectors.

Table 3 provides an overview of each participant's experience by illustrating the pseudonyms given to each participant, the organisation, and their position within.

Table 3. Overview of the participants interviewed

Pseudonym	**Position**	**Industry**	**Organisation size**
Alpha	Cybersecurity professional	Public healthcare	Small
Bravo	Data protection expert	City government	Medium
Charlie	Cybersecurity professional	ICT	Small
Delta	Data protection expert	ICT	Medium
Echo	Cybersecurity professional	Social services	Small
Foxtrot	Data protection expert	IT Services	Small
Golf	Data protection expert	Professional services	Medium

All of the data protection experts agreed that there is an insufficient level of data protection measures implemented within organisations, both in the public and private

sectors. Additionally, they expressed that AKI, which is responsible for overseeing data protection had not taken adequate or severe enough measures to improve that.

Foxtrot brought up that there isn't enough intrinsic motivation in data protection experts, resulting in a low enforcement level, suggesting a lack of resources as a possible reason.

Bravo and Delta echoed the same sentiment, saying that the person responsible for implementing and managing sufficient data protection measures and processes is expected to do most of the work.

Similarly, cybersecurity professionals echoed similar concerns in their field, noting that the current level of cybersecurity and cyber resilience falls short of effectively protecting institutions from cyber threats and attacks.

Moreover, local governments and other small organisations rely heavily on service providers for their internal IT and cybersecurity services.

Another prevalent theme throughout all interviews was the notable division between cybersecurity and data protection within most organisations, evident in processes and interpersonal communications.

Echo revealed that a significant proportion of data protection experts do not understand how systems and databases work. They often focus excessively on legal frameworks rather than extrapolating the guidelines provided by legislation.

Delta and Golf, however, expressed a slightly differing perspective, implying a disconnection between data protection and cybersecurity professionals to the extent that collaboration between the two may not even be registered as necessary. Furthermore, they highlighted a lack of coordination and mutual understanding between them, stemming from differences in educational backgrounds and viewpoints.

When questioned about current cybersecurity processes, there was another consensus, this time across most cybersecurity and data protection experts, outlining that most organisations perceive cybersecurity standards as burdensome obligations rather than strategic frameworks for enhancing data protection and security.

Responsibility and accountability for information assets across institutions were almost non-existent, with the bulk of accountability often delegated to third-party service providers or the individual responsible for the cybersecurity management and implementation.

5 Development of Process

Based on the information gathered during the literature review and analysis of conducted interviews, four main aspects are addressed by the development of this process:

1. Insufficient collaboration and cooperation between cybersecurity and data protection.
2. Underutilisation of information gathered regarding business assets.
3. Limited awareness and concern among developers and other technical stakeholders.
4. Lack of resources.

This process will exclusively focus on IT business assets and will not address physical or organisational business assets. It is designed to strengthen cybersecurity and security management practices within varying-sized organisations across sectors and industries.

The design allows businesses to select and implement cybersecurity management standards that align with their business needs, preferences, and financial constraints. This enables institutions to take a proactive approach to addressing threats and safeguarding their digital assets and data.

This process involves the roles of Asset Owner, Security Expert, Data Protection Expert, and Developer / System Administrator, whose responsibilities are outlined in Table 4.

The objective in determining necessary roles was to minimise the utilisation of human resources while ensuring the inclusion of all necessary aspects to account for the lack of capital in smaller organisations.

Furthermore, in this process, the Developer / System Administrator is depicted as an internal stakeholder; however, the same activities and responsibilities could be applied if the technical stakeholders were external contractors.

Table 4. Roles and responsibilities within the process.

Role	Responsibility
Asset Owner	Accountable for the information, processes, and relevant stakeholders related to the business assets. Their responsibility is to maintain documentation, determine necessary resources, and ensure the business continuity objectives.
Security Expert	Responsible for the implementation, maintenance, and monitoring of the ISMS.
Data Protection Expert	Responsible for assuring the protection and privacy of personal or sensitive data, and compliance with GDPR.
Developer / System Administrator	Is involved with the development, maintenance, and/or improvement of the business asset.

It will establish clear communication channels between the related parties, clearly outlining the roles and what aspects they are responsible for. This will ensure that the security measures and controls are aligned with necessary data protection requirements and vice versa, as well as supporting the organisation's business continuity goals.

Business continuity objectives can be determined through the business impact analysis (BIA), where different scenarios are described according to their impact on the CIA and their effect on the business functions. This provides valuable inputs for the risk management and DPIA processes (see Figure 5).

Moreover, the information gathered during the BIA process will allow the organisation to evaluate and define the assets' recovery point and time objectives and determine the minimum business continuity requirements.

This process will also foster a more collaborative and proactive approach. Through it, vulnerabilities and possible oversights can be identified and rectified before the business asset is implemented, reducing the likelihood of an exploitation of a known vulnerability due to bad practices.

For example, in compliance with regulations such as the GDPR, organisations must implement logging when handling personal or other sensitive data. These logs containing access and activity information must be retained for a specified time, depending on the

regulation. By incorporating this process, the Asset Owner will be informed of that requirement prior to the development and implementation of the asset. This ensures that the asset is equipped to generate the required logs upon deployment, hence maintaining compliance and allowing monitoring and auditing of data access and usage [25].

Moreover, it allows for a joint risk management process, where risks related to personal data processing are managed along with cybersecurity risks, providing a clear and comprehensive summary and overview of all risks associated with a particular business asset.

When developing this process, it was important to find ways to reuse the information that relevant stakeholders had already disclosed to strengthen cybersecurity and data protection measures. For instance, documenting and associating the vendor data gathered during the DPIA with the asset so that it can later be used in the cybersecurity processes and the governing of partner information.

Furthermore, the association of vendors with specific business assets offers various advantages. Beyond providing an apprehensible overview of the type of data shared with third parties and ensuring regulatory compliance, these links can streamline incident response efforts. For example, in case of a supply chain attack or compromise, having clear visibility into the links between business assets and partner entities allows for a more efficient prioritisation and quarantine of affected systems, databases and/or applications.

Lastly, the integration of two separate processes – cybersecurity and data protection – allows SMEs with limited expertise and resources to comprehend all the steps needed to meet baseline requirements for cyber resilience and regulatory compliance. This approach provides a high-level guideline for implementing data protection and security processes, producing a more comprehensive and accessible approach for safeguarding IT assets and data against cyber threats.

In addition to compliance with the GDPR, this process covers baseline security measures set forth by NIS2, such as risk assessment and management, supply chain governance and security, business continuity, and overview and proper cataloguing of business assets [5].

Overall, this process design addresses the challenges mentioned at the beginning of this chapter by fostering collaboration between relevant stakeholders, optimising the use of

information already available about a business asset, and improving the awareness and involvement of technical stakeholders. Continuous improvement and strategic monitoring could strengthen the organisation's overall cybersecurity and data protection posture, helping manage risks, and ensure compliance with relevant regulations and standards.

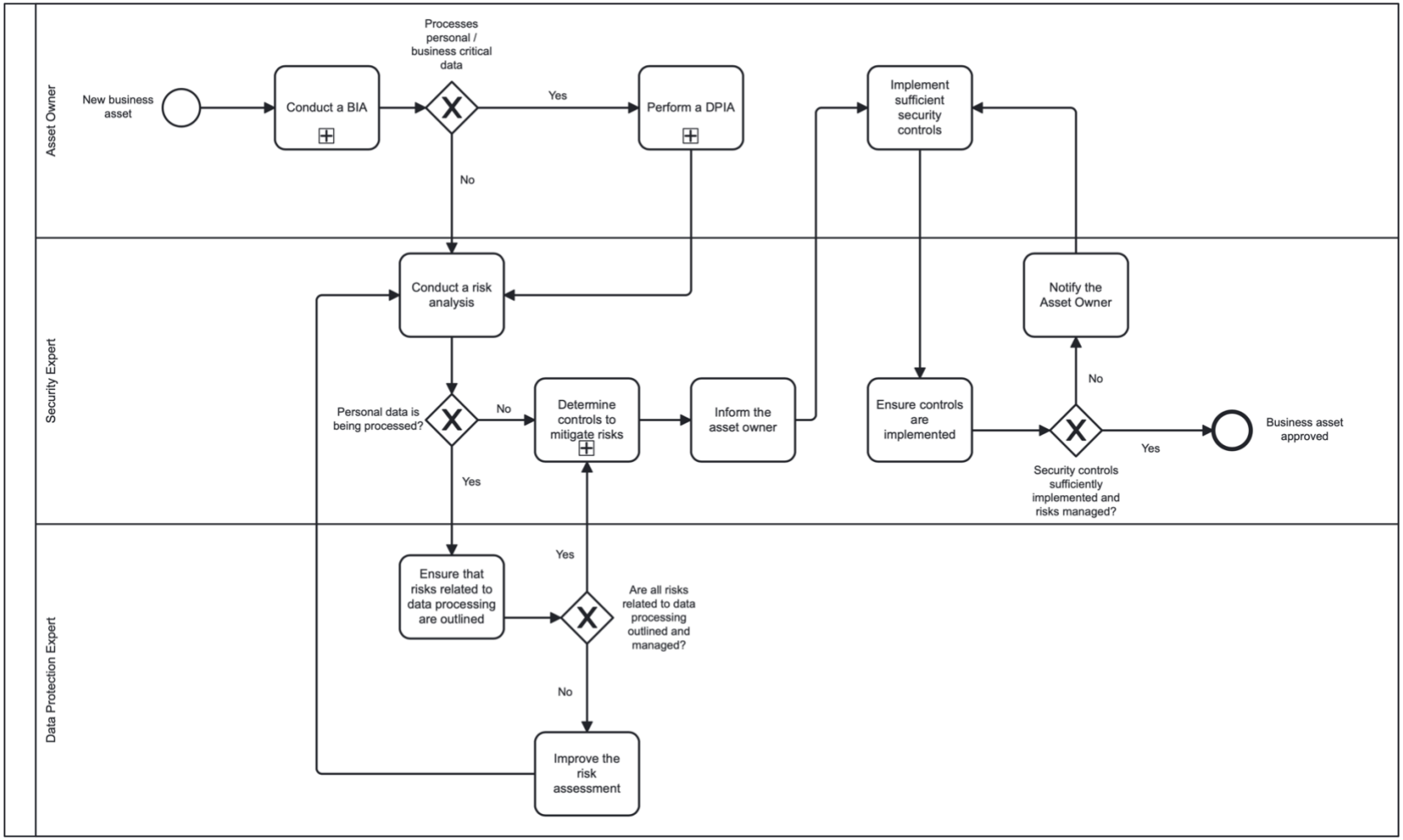

Figure 3. The main process integrating cybersecurity and data protection processes.

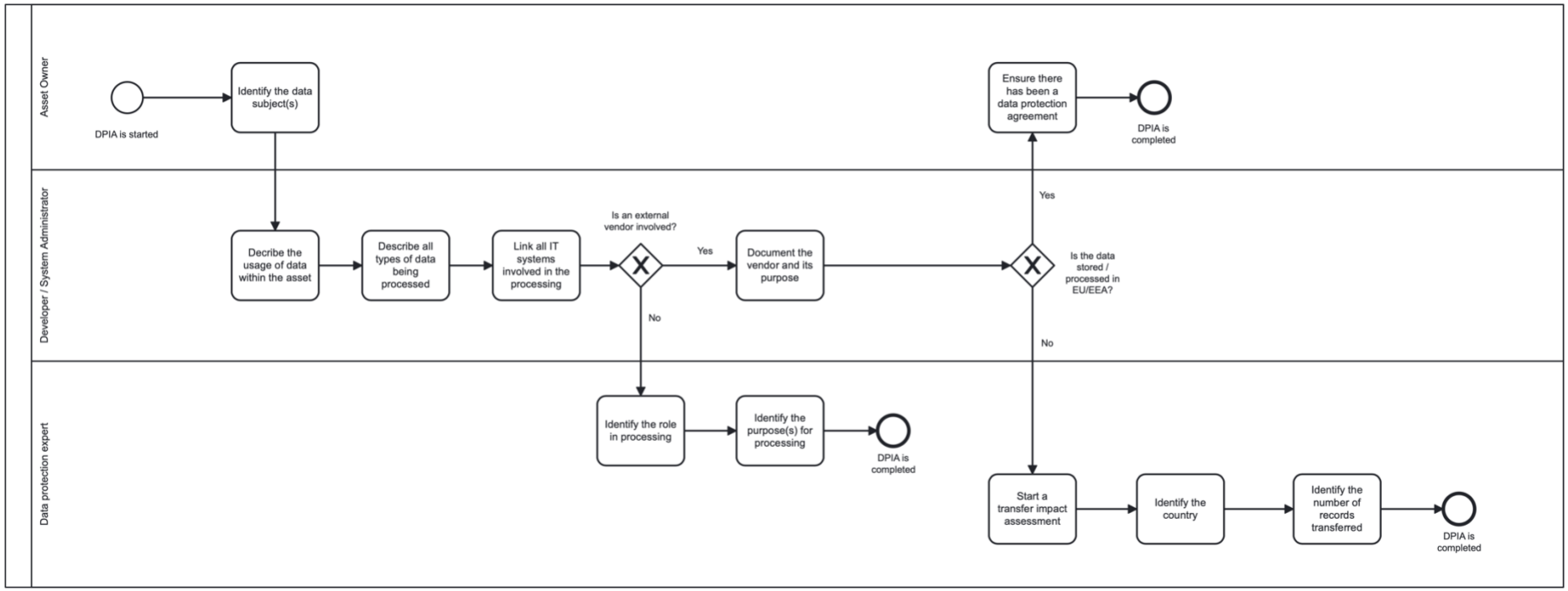

Figure 4. DPIA sub-process.

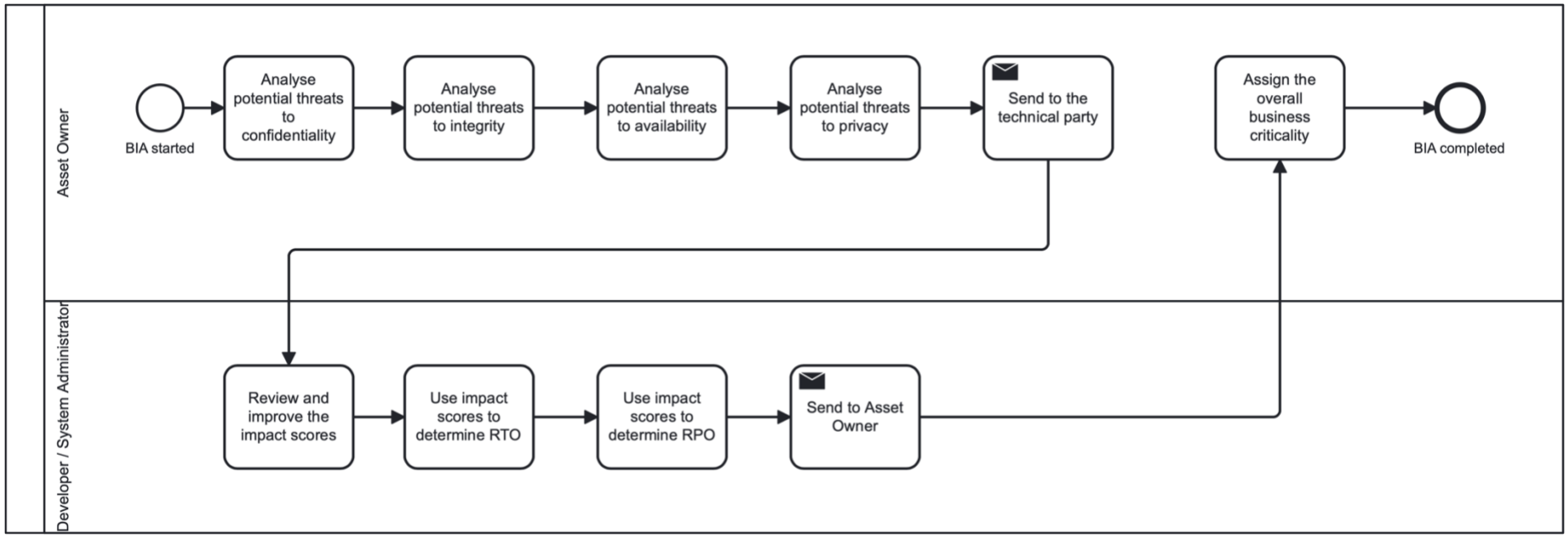

Figure 5. BIA sub-process.

6 Conclusion

This thesis focused on exploring varying cybersecurity and data protection processes, considering the existing threat landscape, the EU's regulatory environment, and distinct challenges faced by SMEs in light of the increasing frequency of data-related incidents. Based on the analysis of these findings, a business process was designed that could be applied independent of the organisation's industry or size.

A combination of expert interviews and an extensive literature review provided a broad, but balanced viewpoint of practical experiences and theoretical foundations that guided the development of the process that bridges the gap between cybersecurity and data protection.

The key findings of this research outlined that SMEs face an increased risk of cyberattacks. There is a lack of cybersecurity and data protection measures in place due to financial constraints, limited resources, and limited understanding among stakeholders.

Furthermore, this thesis contributes to the broader understanding of the requirements set forth by relevant EU legislation, such as NIS2 and GDPR, and highlights the importance of implementing a proactive approach to cybersecurity to lower the risks associated with data breaches.

By prioritising cybersecurity and data protection measures, organisations of any size can more efficiently safeguard their information assets and improve their cybersecurity posture, therefore ensuring the confidentiality, integrity, and availability of their data.

References

[1] F. H. Cate, C. Kuner, D. J. B. Svantesson, O. Lynskey, and C. Millard, "The rise of cybersecurity and its impact on data protection," *Int. Data Priv. Law*, vol. 7, no. 2, pp. 73–75, May 2017, doi: 10.1093/idpl/ipx009.

[2] A. Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1–5. doi: 10.1109/CyberSA49311.2020.9139638.

[3] European Union Agency for Cybersecurity, *ENISA threat landscape 2023*. LU: Publications Office, 2023. Accessed: Apr. 13, 2024. [Online]. Available: https://data.europa.eu/doi/10.2824/782573

[4] International Organisation for Standardisation, "Information security, cybersecurity and privacy protection — Information security controls." International Organisation for Standardisation, 2022. [Online]. Available: https://www.iso.org/standard/75652.html

[5] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)," *Off. J. Eur. Union*, vol. OJ L 333, pp. 80–152, Dec. 2022.

[6] N. Walliman, *Research Methods: The Basics*. Routledge, 2011.

[7] N. Bergen and R. Labonté, "'Everything Is Perfect, and We Have No Problems': Detecting and Limiting Social Desirability Bias in Qualitative Research," *Qual. Health Res.*, vol. 30, no. 5, pp. 783–792, Apr. 2020, doi: 10.1177/1049732319889354.

[8] "Business Process Model and Notation (BPMN), Version 2.0," 2011, Accessed: Mar. 24, 2024. [Online]. Available: https://www.omg.org/spec/BPMN/2.0/PDF

[9] L. Aldin and S. de Cesare, "A Comparative Analysis of Business Process Modelling Techniques," *UK Acad. Inf. Syst.*, 2009.

[10] M. Chinosi and A. Trombetta, "BPMN: An introduction to the standard," *Comput. Stand. Interfaces*, vol. 34, no. 1, pp. 124–134, Jan. 2012, doi: 10.1016/j.csi.2011.06.002.

[11] Ernst & Young, "Protsessianalüüsi Käsiraamat." Majandus- ja Kommunikatsiooniministeerium, 2012. [Online]. Available: https://digiriik.eesti.ee/juhend/protsessianaluusi-kasiraamat

[12] A. Althonayan and A. Andronache, "Shifting from Information Security towards a Cybersecurity Paradigm," in *Proceedings of the 2018 10th International Conference on Information Management and Engineering*, Salford United Kingdom: ACM, Sep. 2018, pp. 68–79. doi: 10.1145/3285957.3285971.

[13] Riigikogu, "Cybersecurity Act," Riigi Teataja. Accessed: Apr. 08, 2024. [Online]. Available: https://www.riigiteataja.ee/en/eli/526082022002/consolide

[14] X. Zhang, M. M. Yadollahi, S. Dadkhah, H. Isah, D.-P. Le, and A. A. Ghorbani, "Data breach: analysis, countermeasures and challenges," *Nt J Inf. Comput. Secur.*, vol. 19, no. Nos. 3/4, pp. 402–442, 2022.

[15] European Commission, "SME definition," Internal Market, Industry, Entrepreneurship and SMEs. Accessed: Mar. 21, 2024. [Online]. Available: https://single-market-economy.ec.europa.eu/smes/sme-definition_en

[16] European Union Agency for Cybersecurity, *Identifying emerging cybersecurity threats and challenges for 2030*. LU: Publications Office, 2023. Accessed: Apr. 14, 2024. [Online]. Available: https://data.europa.eu/doi/10.2824/117542
[17] S. E. Madnick, "The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase," Dec. 2023.
[18] T. Rahman, R. Rohan, D. Pal, and P. Kanthamanon, "Human Factors in Cybersecurity: A Scoping Review," in *The 12th International Conference on Advances in Information Technology*, Bangkok Thailand: ACM, Jun. 2021, pp. 1–11. doi: 10.1145/3468784.3468789.
[19] T. Lopez, H. Sharp, T. Tun, A. Bandara, M. Levine, and B. Nuseibeh, "'Hopefully We Are Mostly Secure': Views on Secure Code in Professional Practice," in *2019 IEEE/ACM 12th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE)*, Montreal, QC, Canada: IEEE, May 2019, pp. 61–68. doi: 10.1109/CHASE.2019.00023.
[20] "What is Data Protection?," SNIA. Accessed: Mar. 15, 2024. [Online]. Available: https://www.snia.org/education/what-is-data-protection
[21] European Union, Ed., *Handbook on European data protection law*, 2018 edition. in Handbook / FRA, European Union Agency for Fundamental Rights. Luxembourg: Publications Office of the European Union, 2018. doi: 10.2811/58814.
[22] "What is Data Privacy?," SNIA. Accessed: Mar. 15, 2024. [Online]. Available: https://www.snia.org/education/what-is-data-privacy
[23] E. Bertino, "Data Security and Privacy: Concepts, Approaches, and Research Directions," in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, Atlanta, GA, USA: IEEE, Jun. 2016, pp. 400–407. doi: 10.1109/COMPSAC.2016.89.
[24] A. Aljeraisy, M. Barati, O. Rana, and C. Perera, "Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective," *ACM Comput Surv*, vol. 1, no. 1, pp. 1–37, 2022.
[25] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Off. J. Eur. Union*, vol. L 119, no. 1, pp. 1–88, Apr. 2016.
[26] International Organisation for Standardisation, "Information security, cybersecurity and privacy protection — Information security management systems - Requirements." International Organisation for Standardisation, 2022. [Online]. Available: https://www.iso.org/standard/27001
[27] Riigi Infosüsteemi Amet, "E-ITS," Eesti Infoturbestandard. Accessed: Apr. 07, 2024. [Online]. Available: https://eits.ria.ee/et/versioon/2023/eits-poohidokumendid/eits-nooude-d-infoturbe-halduse-suesteemile
[28] Riigi Infosüsteemi Amet, "Tutvustus," Eesti Infoturbestandard. Accessed: May 08, 2024. [Online]. Available: https://eits.ria.ee/et/avalehe-menueue/tutvustus/standardist
[29] Riigi Infosüsteemi Amet, "Eesti infoturbestandard." Jan. 08, 2024. [Online]. Available: https://eits.ria.ee/api/2/home/asset/Lisa2_%20E_ITS_Etalonturbe%20kataloog_FINAL-240108.pdf

[30] Andmekaitse Inspektsioon, “Mõjuhinnangust ja eelkonsulteerimisest,” Andmekaitse Inspektsioon. Accessed: Apr. 08, 2024. [Online]. Available: https://www.aki.ee/uudised/mojuhinnangust-ja-eelkonsulteerimisest
[31] L. Cheng, F. Liu, and D. (Daphne) Yao, “Enterprise data breach: causes, challenges, prevention, and future directions,” *WIREs Data Min. Knowl. Discov.*, vol. 7, no. 5, p. e1211, Sep. 2017, doi: 10.1002/widm.1211.
[32] IBM Security, “Cost of a Data Breach Report 2023,” *IBM*, 2023.
[33] I. Jibilian and K. Canales, “The US is readying sanctions against Russia over the SolarWinds cyber attack. Here’s a simple explanation of how the massive hack happened and why it’s such a big deal,” Business Insider. Accessed: Mar. 21, 2024. [Online]. Available: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12
[34] Fortinet, “SolarWinds Supply Chain Attack,” Fortinet. Accessed: Mar. 21, 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack
[35] M. Karyda and L. Mitrou, “Data Breach Notification: Issues and Challenges For Security Management,” *Tenth Mediterr. Conf. Inf. Syst. MCIS*, pp. 1–12, Sep. 2016.
[36] Riigi Infosüsteemi Amet, “‘Uksest, kust sisse annab murda, sisse ka minnakse.’ Miks toetab RIA ettevõtete küberturvalisust 60 000 euroga?,” DigiPRO. Accessed: Apr. 08, 2024. [Online]. Available: https://digipro.geenius.ee/blogi/turvalise-e-riigi-blogi/uksest-kust-sisse-annab-murda-sisse-ka-minnakse-miks-toetab-ria-ettevotete-kuberturvalisust-60-000-euroga/
[37] Andmekaitse Inspektsioon, “Strateegia ja missioon,” Andmekaitse Inspektsioon. Accessed: Mar. 19, 2024. [Online]. Available: https://www.aki.ee/meist/aki/strateegia-ja-missioon
[38] Andmekaitse Inspektsioon, “Statistics,” Andmekaitse Inspektsioon. Accessed: Mar. 19, 2024. [Online]. Available: https://www.aki.ee/en/inspectorate-news-information-dpo-s/statistics
[39] “Allium UPI OÜ,” e-Äriregister. Accessed: Apr. 01, 2024. [Online]. Available: https://ariregister.rik.ee/est/company/11331786/Allium-UPI-O%C3%9C
[40] “Asper Biogene OÜ,” e-Äriregister. Accessed: Apr. 01, 2024. [Online]. Available: https://ariregister.rik.ee/est/company/14265334/Asper-Biogene-O%C3%9C
[41] ERR, “Andmekaitse: Asper Biogene andmelekkes on ka näiteks isadusteste,” ERR. Accessed: Mar. 21, 2024. [Online]. Available: https://www.err.ee/1609195564/andmekaitse-asper-biogene-andmelekkes-on-ka-naiteks-isadusteste
[42] M. Tooming, “At least one case of extortion reported following Asper Biogene data leak,” ERR. Accessed: Mar. 19, 2024. [Online]. Available: https://news.err.ee/1609204528/at-least-one-case-of-extortion-reported-following-asper-biogene-data-leak
[43] K. Põlendik, “Cybercriminals steal data of around 700,000 Apotheka pharmacy customers,” ERR. Accessed: Mar. 19, 2024. [Online]. Available: https://news.err.ee/1609302096/cybercriminals-steal-data-of-around-700-000-apotheka-pharmacy-customers

Appendix 1 – Non-exclusive license for reproduction and publication of a graduation thesis[1]

I, Maria Schlosser,

1. Grant Tallinn University of Technology free license (non-exclusive license) for my thesis “Designing a Comprehensive Process Bridging the Gap Between Cybersecurity and Data Privacy”, supervised by Kristjan Karmo and Katrin Vernik.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive license.
3. I confirm that granting the non-exclusive license does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

13.05.2024

1 The non-exclusive license is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive license, the non-exclusive license shall not be valid for the period.