Data protection for e-invoicing in Poland: Case Pagero

Adrianna Pytka

2022 Laurea

Laurea University of Applied Sciences

Data protection for e-invoicing in Poland: Case Pagero

Adrianna Pytka
Safety, Security and Risk Management
Thesis
December, 2022

Laurea University of Applied Sciences **Abstract**
Safety, Security and Risk Management
Bachelor's Degree

Adrianna Pytka

Data protection for e-invoicing in Poland: Case Pagero

Year 2022 Number of pages 35

This thesis was completed for Pagero, a company that specializes in IT consulting and solution delivery. It creates a platform where other businesses can exchange all kinds of business documents digitally. From January 2024, taxpayers in Poland will have to use the National System of e-Invoice to make structured electronic invoices. This is why Pagero saw a big opportunity to find customers in the Polish market.

The thesis is a qualitative research study. The objectives are to determine whether Pagero complies with Polish data protection legislation and to determine the potential benefits of using Pagero services in Poland. Methods included a review of the literature and a semi-structured interview. Different research papers or publications from the field of data protection were selected. They were analyzed through thematic analysis as well as an interview.

The results show that Pagero has been well organized in terms of data protection. Customers can benefit from the company because they can join the platform regardless of size, business, or service usage. As a suggestion for a company, it could be a booklet created about data protection in Poland for sales or commercial purposes.

Keywords: Data security, Data Protection, E-invoicing, E-invoicing in Poland

Table ofcontents

1 Introduction 5
1.1 Information about company and my role 6
1.2 Research question of the study 6
2 Data protection used for e-invoicing in Poland 7
2.1 Data Security and Data Protection 8
2.1.1 General Data Protection Regulation 9
2.1.2 The International Organization for Standardization / International Electrotechnical Commission 27001 (ISO/IEC 27001) 10
2.1.3 The International Standard for Reporting over Non-Financial Information (ISAE3000 SOC2 Type2) 11
2.1.4 Polish Telecommunication Act 12
2.2 E-invoicing 14
2.2.1 History of e-invoicing evolution 16
2.2.2 Polish e-invoicing reform 17
3 Methodology 18
3.1 Literature review 19
3.1.1 Database and selection of the material 20
3.1.2 Analysis of the literature review 20
3.2 Interview 21
3.2.1 Interviewee 23
3.2.2 Analysis of the interview material 24
4 Results 25
5 Conclusion 27
References 29
Figures 33
Tables 33
Appendices 34

1 Introduction

Data protection is of the utmost importance in documents such as electronic invoices. There are a wide variety of dangers that can affect companies and other types of entities. One of these would be hacking of a database. Businesses must have a good understanding of how to protect not only their own information but also the information of their customers.

The protection of personal information is governed by several organizations, both domestic and international. The use of paper is made more secure by the passage of laws and regulations at the state level. A large number of companies are still using paper invoices. However, businesses are making efforts to get away from this by digitizing their records to a substantial degree. This is a step toward making the switch to energy sources that are better for the environment and protect data. (Endresen 2021.)

Poland is one of the countries that has lately initiated reforms that have shifted away from the usage of paper invoices towards electronic ones. Ministry of Finance in Poland announced that every business in this nation will be compelled to switch to using electronic invoices beginning in January 2024 (Ministry of Finance in Poland 2022). The situation that existed in the Polish market prompted several companies, including Pagero, to extend their operations in Poland. Pagero specializes in the automation of processes and assists customers in digitizing their documents.

This is a research project aimed at checking whether the services provided by Pagero comply with the Polish law on the protection of personal data in e-invoicing. For this purpose, the literature on the subject of personal data protection and invoicing is analyzed, as are the regulations in force in Poland and Pagero's compliance with the requirements of the Polish market. In order to collect specific information on data protection, the Data Protection Officer from Pagero is interviewed. In other words, about how difficult it is to get into the Polish market and how the company works to comply with Polish data protection laws.

The primary objective of this thesis, however, is to determine whether Pagero, which provides services in Poland, complies with local data protection regulations for e-invoicing. This allows to discover potential benefits from using Pagero services in Poland. Customers interested in learning more about Pagero's data security measures and how they operate in Poland may find the information below useful. Furthermore, Pagero employees can gain additional experience and apply it to their daily work.

The general information about the company and the thesis will be supplied at the beginning of this thesis. The first chapter also addresses the issue of the research question. The second

chapter contains material collected from a literature review, such as legal documents and various types of data protection legislation. There is additional information on the history and development of e-invoicing. There seems to be details about the amendment of e-invoicing system that has been implemented in Poland. In the third chapter, the methodology is described, followed by the results. The conclusion contains a summary of the entire material.

1.1 Information about company and my role

Pagero is a company that specializes in the delivery of information technology services as well as information technology consultancy. It began operations in the year 2000 and currently has its headquarters in Gothenburg, which is in Sweden. It is functioning in more than 30 nations in the world. The fundamental objective of Pagero is to establish its network platform as the most effective and secure mechanism for the exchange of business documents and the flow of information between businesses during the purchase-payment processes as well as payment orders. (Pagero 2022.)

In other words, Pagero creates networks with businesses to facilitate the digital and automatic interchange of business documents such as orders, invoices, payment instructions, and other documents. Companies, regardless of the technologies they use or their level of digital capability, can connect with the platform. It is compatible with each company, irrespective of the type of enterprise that they manage. Each of the systems can be smoothly merged with any other system. Pagero ensures that everything complies with the regulations in every local market. (Pagero 2022.)

My employment with Pagero began in January 2022. My primary responsibility is to help clients who speak Polish. As part of my job, I'm expected to help Polish customers who are having issues with the Pagero services they are using and instruct them on how to make the best use of the platform in order to accomplish their goals. Customers have the option of submitting their concerns using the customer portal or contacting the company by phone. Because the organization places a strong emphasis on providing superior support to customers, it does so around the clock.

1.2 Research question of the study

From January 1, 2024, taxpayers in Poland are required to generate structured electronic invoices (e-invoices) via the National System of e-Invoice (Krajowy System e-Faktur, KSeF). When preparing structured invoices, it should be done in accordance with the invoice template that was developed by the Ministry of Finance and included in local finance and accounting programs for business owners. After being issued, the invoice is transferred from the financial and accounting system to the central database of the Ministry of Finance using the Application Programming Interface (API) as a communication channel. After submission,

the invoice is made available in this system for the supplier to retrieve. (Ministry of Finance in Poland 2022.)

On the basis of the aforementioned considerations, it is possible to define a research problem that is related to the adaptation of Pagero to the requirements of the National E-invoicing System (KSeF) in the field of electronic invoice format while simultaneously ensuring data protection in accordance with the law that is applicable in Poland. The key problem in this work is whether Pagero meets the requirements for data protection in electronic invoicing in Poland. Based on the research problem, the research question can be formed:

"How are Pagero's services compliant with Polish law and regulations regarding data protection for e-invoicing? "

The scope of the topic has been narrowed to the information that is gathered is restricted to that which is applicable to the Polish laws governing data protection and electronic invoicing. What steps Pagero has taken to make sure it meets data protection standards for electronic invoicing in the Polish market. There is no information in this work about other countries and how their data protection is established regarding e-invoicing.

By answering the research question, it will be feasible to demonstrate how the clients could benefit from Pagero's services regarding data privacy. Customers in Poland who are interested in learning how the security of their data can be ensured when utilizing Pagero's services might benefit from having this information. Since January 2022, Pagero has been operating in Poland. This may also prove useful for Pagero in the future, when the company plans to enter a market that is similar to that in Poland.

2 Data protection used for e-invoicing in Poland

There is a likelihood that some parts of electronic invoicing will include information that can be used to identify a person. Name, address, phone number, e-mail address, or any other information that helps to identify the person could be included. This perchance sometimes involves confidential information. For example, the information may consist of the type of medical treatment, psychological treatment, or social services that were given, and this information is linked (or can be linked) to the names of the people who received these treatments or services. (Buttarelli 2013.)

It is important to recognize how crucial the protection of data is by looking at the examples that have been presented above. It preserves not just the personal information of individuals, but also that of businesses and organizations against illegal acts such as hacking, scamming or identity theft. This chapter covers topics relevant to the data protection of electronic

invoicing in Poland. What kind of data security measures are in Poland, and what kinds of laws and regulations control electronic invoicing. What types of certifications does Pagero need to have in order to be compliant with the requirements for electronic invoicing in Poland regarding the safety of customer data? There is additional explanation of the history of invoicing, as well as a description of the Polish mandate for electronic invoices.

2.1 Data Security and Data Protection

Data security is the practice of keeping digital information safe from being stolen or accessed by people who should not be able to. It is a concept that includes every part of information security, from the physical security of hardware and storage devices to administrative and access controls and the logical security of software applications. It also includes the policies and procedures of the organization. Strong data security strategies, when used correctly, protect an organization's information assets from cybercriminals. They also protect against insider threats and human error, which are still some of the most common reasons for data breaches today. Data security means that using tools and technologies makes it easier for an organization to see where its most valuable data is stored and how it is used. In an ideal world, these tools would be able to protect sensitive files with things like encryption, data masking, and redaction, as well as automate reporting to make audits and meeting regulatory requirements easier. (IBM 2022.)

Data security is required to handle data securely by implementing "appropriate technical and organizational measures." Technical measures mean anything from requiring your employees to use two-factor authentication on accounts where personal data is stored to contracting with cloud providers that use end-to-end encryption. Organizational measures are things like staff training, adding a data privacy policy to the employee handbook, or limiting access to personal data to only those employees in your organization who need it. If there has been a data breach, there are 72 hours to tell the data subjects or face penalties. It is important to remember that this requirement may not have to be met if technological safeguards like encryption are used to make the data useless to an attacker. (Wolford 2022.)

In Poland, the Polish Data Protection Office (Urząd Ochrony Danych Osobowych, UODO) is a main regulator for data protection. The General Data Protection Regulation (GDPR) is the main law that controls data protection in Poland. It has been implemented into The Act of 10 May 2018 on the Protection of the Personal Data (Ogólne Rozporządzenie o Ochronie Danych RODO). (UODO 2019.)

Data protection is a process of keeping important information safe from being changed, lost, or stolen. The most important tools for protecting data are backup and recovery, but there are many other tools as well. Usually, an organization will name a data protection officer who oversees finding the data that needs to be protected and coming up with a set of rules to

make sure that the data can be recovered if it is lost, overwritten, or damaged. Data protection policies protect data in a way that is in line with an organization's service-level agreements, especially when it comes to recovery point objectives (RPOs) and recovery time objectives (RTOs). (Posey 2021.)

Data protection must be considered when making any new product or an activity. This is covered in GDPR in Article 25. For example, if a company has released a new app, it is important to think about what personal information this app could get from the users. Also, how to reduce the amount of information and how to keep it safe with the newest technology. (Wolford 2022.)

Terms "protection" and "security" are sometimes used interchangeably, although there are important distinctions between them. The term "data protection" is used to describe the process of protecting the fundamental human rights of individuals. While data security is what you put in place to prevent unauthorized people from viewing or sharing your information, the former is what people usually think of first. Protecting the data from unauthorized access that could lead to data compromise, corruption, or erasure is the goal of data security. (Digital Sense 2022) The following material elaborates on the fundamental factors like acts, regulations, standards, and laws that have been taken into account for data protection for e-invoicing in Poland and how it is with case of Pagero.

2.1.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) was approved by the EU Council and Parliament in April 2016, and it became legally binding across all Eu Members in May 2018. In Poland, the Ministry of Digital affairs worked on the regulation and from May 2018 the General Data Protection Regulation (in Polish - Ogólne rozporządzenie o ochronie danych RODO) formally went into effect. The General Data Protection Regulation (GDPR) is a document that establishes rules for organizations as well as for Member Countries and makes provisions for an EU Data Protection Commission. This chapter's goal is to provide a concise summary of the most important aspects of compliance with the General Data Protection Regulation.

By definition from General Data Privacy Regulation (2016), this regulation establishes guidelines for the protection of individuals when processing personal data, as well as guidelines for the free flow of personal data. The fundamental rights and freedoms of natural people — in particular, their right to privacy — are safeguarded by this regulation. The free movement of personal data within the Union shall not be restricted or prohibited for reasons related to the protection of natural persons in relation to the processing of personal data. (General Data Privacy Regulation 2016) Article 5 of the GDPR defines the six principles that should be applied to any collection or processing of personal data. These principles should be

considered whenever personal data is collected or processed. Processing of personal data must comply with all applicable laws and be conducted in a transparent and truthful manner. Only for coherent and legally permissible purposes may an individual's personal data be acquired. Data pertaining to individuals must be accurate, relevant, and restricted to what is required for processing. Information related to individuals must be exact and always kept current. When personal information is stored for a period that is longer than what is required for processing, it must be done so in a way that renders the data subject anonymous. Processing of personally identifiable information must take place in a way that guarantees the data's privacy and safety. (Calder 2018.)

2.1.2 The International Organization for Standardization / International Electrotechnical Commission 27001 (ISO/IEC 27001)

When it comes to personal information management systems (PIMS), the GDPR demands more than just implementation. Organizations must comply with the following 14-point mandate. A process for routinely testing, assessing, and evaluating the efficacy of technical and organizational measures for ensuring the security of processing. The capacity to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services. The capability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. Consequently, it is imperative that businesses adopt a more all-encompassing strategy for information security, one that addresses not only the processing systems and services but also security, continuity, and continuous security testing (primarily in the form of penetration testing), and data and privacy protection as part of "business as usual."

ISO/IEC 27001 is a standard for management systems in the field of information security and is recognized worldwide. Using industry standards as its guide, it details what should be included in an Information Security Management System (ISMS). It is applicable to businesses of any size and may be utilized with any technology or solution. It specifies what must be done to secure information but leaves it up to individual organizations to decide how best to put those specifications into practice considering their own objectives and tolerance for risk. The information security framework presented here can also be utilized to earn a recognized international certification. More and more contracts that involve sensitive information now require this kind of certification to show that the company cares about data security. (General Data Protection Regulation 2016.)

Certified level of compliance with ISO/IEC 27001 by an accredited and trustworthy certificate authority is entirely voluntary but is increasingly demanded from suppliers and business partners by organizations that are concerned about the security of their information and information risks throughout the supply chain/network. The certificate demonstrates that the

organization takes information security management seriously and has marketing potential and brand value. (ISO/IEC 27001: 2013; ISO/IEC 2022:2022.)

2.1.3 The International Standard for Reporting over Non-Financial Information (ISAE3000 SOC2 Type2)

The International Standards for Assurance Engagements (ISAE 3000) is a set of guidelines for establishing trust in data that is not non - financial. Everything from sustainability and governance to network security can be included in the standard. The topic determines the standards used to evaluate the work. Technical security, availability, continuity, and confidentiality are all examples of common control areas in the context of discussing information security. There are two reports accepted by ISAE 3000. Type 1 report guarantees status of control for a specific date. Type 2 guarantees the design, implementation, and control for a specific period, which is usually one year. (Anton 2022.)

Systems and Organizational Controls (SOC) reports are the results of an independent auditor's examination of a company's policies and practices as they pertain to protecting the privacy of their clients' information. A company seeking SOC 2 accreditation is required to follow the Committee of Sponsoring Organizations (COSO) principles which are presented in Figure 1. The seventeen Principles of Internal Control from Figure 1. highlight various categories, including environmental control, risk assessment, control actions, information and communication, and monitoring activities. Each of the principles contains a variety of responsibilities. These guidelines that the business has safeguards in place to protect its data, that only authorized personnel have access to sensitive information, and that risks are minimized by regular training, system monitoring, and review of business associates and outside vendors. (LeadDesk 2022.)

CONTROL ENVIRONMENT	RISK ASSESMENT	CONTROL ACTIVITIES	INFORMATION AND COMMUNICATION	MONITORING ACTIVITIES
• Demonstrates commitment to integrity and ethical values. • Exercises oversight responsibility. • Establishes structure, authority, and responsibility. • Demonstrates commitment to componence. • Enforces accountability.	• Specifies suitable objectives. • Identifies and analyses risk. • Assesses fraud risks. • Identifies and analyses significant change.	• Selects and develops control activities. • Selects and develops general controls over technology. • Develops through policies and procedures.	• Uses relevant quality information. • Communicates internally. • Communicates externally.	• Conducts ongoing and/or separate evaluation. • Evaluates and communicates deficiencies.

Figure 1. COSO's 17 Principles of Internal Control (LeadDesk 2022)

Both SOC 2 and ISO/IEC 27001 provide consumers and stakeholders with the assurance that their data is secure. As a result, there is considerable overlap between the controls of each framework, as they both handle the confidentiality, availability, and integrity of information. They both demand an independent review of security procedures and strive to build confidence in the customer base by mitigating information security risks. Organizations might benefit from obtaining both SOC 2 and ISO/IEC 27001 as both are generally recognized certifications. (DataGuard 2022)

However, as seen in Table 1. SOC 2 and ISO/IEC 27001, differ in several aspects. Table 1 indicates that SOC 2 is more applicable to organizations who have already published a report on their security infrastructure and information security management system (ISMS). It presents also that in SOC 2 the majority of the company's clients are from North America. ISO/IEC 27001, on the other hand, is utilized for international information security and clients. The organization does not have a management structure for information security and would like to establish one, so in this case ISO/IEC 27001 should be used again.

	SOC 2	ISO/IEC 27001
Use	For a current report on the efficacy of information security framework.	To adhere to an international standard of information security.
Information security management system	If there is already an established information security management system (ISMS).	If a company wants to establish an information security management system (ISMS).
Process	For a less demanding certification process.	For an extensive audit process.
Geographical scope	If company have mainly North American clientele.	If company have international clientele.

Table 1. Differences between SOC 2 vs. ISO/IEC 27001 (DataGuard 2022)

2.1.4 Polish Telecommunication Act

The Telecommunication Act (In Polish – Prawo telekomunikacyjne) controls marketing calls and the transmission of marketing information via telecommunications terminal equipment in

Poland. This includes SMS/MMS communications, emails, and phone calls, even those generated by an automated calling system. The Telecommunications Act mandates that end-user consent be obtained separately for the transmission of marketing information through telecommunications terminal equipment and for marketing calls (including via automated calling systems). The consent must comply with the GDPR's standards. To conduct marketing activities in full compliance with the Act on Electronic Services and the Telecommunications Act, two separate consents are required (one for sending marketing information and another for the use of telecommunications terminal equipment and automated calling systems), in addition to any consent required from a data protection standpoint (according to the interpretations of the UODO and the Office of Electronic Communication). However, this is typically not the case. Typically, organizations gather only a single permission for marketing communications or specialized communication channels. (Kowalczuk-Pakula, Jaraczewska & Stępień 2022.)

The telecommunications law is outlined in the Telecommunications Law Act of 2004, as modified. Its purpose is to provide the environment for fostering equal competition among providers of telecommunications services, as well as to construct the infrastructure necessary to offer customers with the benefits coming from services of varying costs and qualities. (Tarnobrzeska 2022.)

The legislation details the performance and management of telecommunications operations, as well as the rights and responsibilities of telecoms businesses and users. The document contains the conditions for engaging in such activity, including the regulation of telecommunications markets, the provision of universal service, the protection of service users, the processing of data in telecommunications, and the safeguarding of telecommunications secrets. (Tarnobrzeska 2022.)

The law of telecommunications is a subset of the law of new technology. The legislation is being revised, and it also incorporates a package of directives from the European Community. Telecommunications undertakings are businesses permitted to engage in the provision of telecommunications networks and associated infrastructure, as well as the supply of telecommunications services. The Telecommunications Law Act specifies in detail the requirements imposed on telecommunications companies. They must, among other things, inform the President of Office of Electronic Communications (in Polish - Urząd Komunikacji Elektronicznej UKE) and end users, guarantee access to telecommunications services, ensure the competitiveness of the telecoms market, and fulfill commitments for the defense and security of the state and the maintenance of public order. Moreover, telecommunications companies must get a listing in the registry of telecommunications companies. The district court will impose a sanction for failure to comply. (Tarnobrzeska 2022.)

2.2 E-invoicing

The exchange of an electronic invoice document between a supplier and a buyer constitutes electronic invoicing. According to Directive 2014/55/EU, an electronic invoice (e-invoice) is a bill that has been issued, transferred, and received in a structured data format that permits its automatic and electronic processing. A structured electronic invoice comprises supplier data in a machine-readable format that may be automatically loaded into the account payable (AP) system of the buyer without requiring user entry. (Directive 2014/55/EU.)

When comparing e-invoices with paper invoices, it is helpful to keep in mind that paper invoices have three features that are so linked that we often do not realize they can be separated. Paper invoices contain data details such as amounts, descriptions, and quantities; portray that data in a visual format, on printed paper, that can be physically read; and have a physical shape that enables human handling and exchange. Digital pictures, PDFs, and other visual digital formats of invoices eliminate the physical element and enable for more efficient handling and archiving than paper invoices. These formats, however, still necessitate manual inspection of the invoice and the entry of its data into AP systems. (Directive 2014/55/EU.)

E-invoices only include structured data and may be imported automatically into AP systems. They do not include a visual representation of the invoice data, although they can be presented temporarily during processing or converted into visual formats. The visual format of e-invoices is secondary, and the goal of automation is not to view the invoice, except in exceptional circumstances. A graphic, human-readable version of the invoice can be created for reading purposes, and it can flow within the structured message, but it is not part of the actual invoice. Therefore, they are not electronic invoices if they are issued in electronic form and then printed and transferred to paper form, or if they are issued in paper form and then scanned, transmitted, or made accessible in electronic form. (Directive 2014/55/EU.)

E-invoicing is frequently confused between several methods of invoice automation. Upon receipt by the buyer, invoice automation by scanning and optical character recognition (OCR) is the digitization of paper-based invoices. Emailing PDF invoices is another kind of automation, although while it eliminates paper, it does not give complete integration. Admitting both systems are frequently referred to as e-invoicing, they are not "genuine" e-invoicing. True e-invoicing entirely automates the invoice capture and receipt process, eliminating the need for data entry by the buyer. This is because invoice information goes straight from the supplier to the buyer's back-office system, necessitating no manual intervention by the buyer. The customer receives bills from its suppliers in forms that were previously agreed upon. The invoices may incorporate authentication and integrity-preserving techniques such as digital signatures and electronic data interchange (EDI). They will be sent

to the buyer in a format that works with their enterprise resource planning (ERP) system and won't be changed for as long as the law requires. (e-InvoicingBasics 2022.)

There are various forms of e-invoices presented in Table 2. Digital invoices can be communicated as files across computer messaging networks, but the features of different types of digital documents determine how they can be handled. A digital invoice has two primary components: the visual component and the data component. The visual aspect enables a human reader to view the content of a document, while the data aspect enables a machine to interpret the document's information. The essential component of visual formats is the visualization of the content, which requires human processing. The primary purpose of data formats is to facilitate computer processing of the data, although certain formats may also support data visualization. (European Commission 2022.)

The Pdf document format is an XML format. However, it is built for the visual presentation of its data as opposed to its automatic reading. It is possible to extract the data content from PDF files, but the procedure is typically unstable and dependent on the visual layout of each invoice. Therefore, the.pdf is included in the above list of visual formats. The primary purpose of data formats is to facilitate computer processing of the data, although certain formats may also support data visualization. (European Commission 2022.)

In accounting systems, data cannot be automatically extracted from documents in unstructured formats. It is possible to describe data in spreadsheets, HTML, and word processor documents such that it can be automatically interpreted by the receiving computer system. Such a definition structures the data, and its automated processing is dependent on the data structure specification. For structured formats, the data can be automatically read into computer systems from the document. The two forms of structured formats are standardized formats (data files based on publicly available specifications EN 16931, UBL, CII, EDIFACT, etc.) and un-standardized formats (internal data files whose structure does not adhere to publicly published specifications). (European Commission 2022.)

Visual digital formats	**Data formats**	
.pdf; digital document format (common in emails)	**Unstructured**	**Structured**
.jpg; .png; .gif (common picture formats)	Spreadsheets; word processors; etc.	Standardised
.tif (common in scanning solutions)	HTML (common in emails and web sites)	Un-standardised

Table 2. Types of digital invoice (European Commission 2022)

To put it in a nutshell, an electronic invoice is an invoice that is sent via electronically and follows a fixed, standardized format. Electronic invoices (or "e-invoices") are invoices sent online that include data that can be directly imported into an accounts payable system. The invoice information is typically displayed graphically. On the other hand, they can be delivered temporarily in the course of processing or converted into visual formats. The use of electronic invoices requires two significant characteristics, one being that the electronic invoice itself be constructed using the correct format. The electronic invoice must be moved from the seller's system to the buyer's system, which brings to the second point. (Medius 2022.)

2.2.1 History of e-invoicing evolution

The first electronic was sent more than 30 years ago via electronic data exchange (EDI). The computer-to-computer exchange of business documents and information is known as electronic data interchange (EDI). EDI is fundamentally a methodology. It is a collection of best practices, standards, protocols, and technology that allow for the free flow of information across multiple organizations — specifically, different firms within the same supply chain. (Data Interchange 2022.)

In the 1960s, the ability of computers to communicate with one another and exchange data cleared the way for what is now known as electronic data interchange (EDI). EDI's "inventor," Edward Guilbert, worked with U.S. Army leaders during the 1948 Berlin airlift to produce standard shipping manifests, which were eventually refined and improved upon in the latter years of the same decade. The system that Guilbert created became the industry standard for electronically communicating freight information. The Holland-American Steamship line utilized Telex connections, which could send a whole page of data in around 2 minutes, to carry Transatlantic shipping manifests as early as 1965. Next, they were converted to a tape file type compatible with personal computers. The Transportation Data Coordinating Committee (TDCC) was established in the 1960s by a consortium of railroad firms in response to the growing use of electronic data interchange (EDI) among marine shipping companies, railroads, airlines, and trucking businesses. Most of the chaos and confusion that followed was caused by the different ways these messengers sent their messages. (McCarthy 2013.)

Abhay Bhusan, from the Massachusetts Institute of Technology, wrote and released the first versions of what would become known as the File Transfer Protocol (FTP) in 1971. It's what makes it possible for a client and a server to share data across the internet. In 1975, the TDCC released its first set of EDI regulations. Edward Guilbert had a major role in formulating and popularizing these norms in the business world. Telenet was established in the same year as the first Value Added Network (VAN) went live. This is the first commercial network to

offer services beyond simple data transmission. In 1978, the TDCC became the Electronic Data Interchange Association (EDI). That same year, American National Standards Institute X12 (ANSI X12) is being founded. The mission of this committee is to create and disseminate EDI standards worldwide. In 1981, ANSI issued the first X12 standards for usage in the financial, pharmaceutical, food, logistics, and transportation sectors. In 1982, Ford, General Motors, Sears, and Kmart were among the first major automakers and retailers to require EDI from their vendors. (Zavorskas 2020.)

The Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) standard was created in 1985 by the United Nations to facilitate the global adoption of electronic data interchange standards. EDIFACT is now widely utilized around the world, apart from the automotive industry, where ANSI X12 standards are followed by most US companies. (Zavorskas 2020.)

By 1991, nearly 12,000 U.S. businesses were using EDI. In 1996, the Uniform Code Council (UCC) established rules for online EDI communication. In 2001, the UCC released the Applicability Statement 2 (AS2) communication standard. In this way, information can be securely transmitted via the web. When Walmart needed to communicate with its vendors, it adopted this standard in 2004. Because of its reliability and high level of security, AS2 has grown in popularity. Over a hundred thousand companies in the US today use EDI to communicate with their suppliers and customers. 90% of Fortune 500 and other companies are represented. A consistent pattern can be seen all around the globe. More and more businesses are ditching on-premises EDI systems in favor of cloud-based alternatives. (Zavorskas 2020.)

2.2.2 Polish e-invoicing reform

The Parliament approved the draft act establishing Poland's National System of e-Invoice (KSeF). The revised regulations went into effect on January 1, 2022, according to the amendment's requirements. The Ministry of Finance indicated that the use of the KSEF would be voluntary from January 1, 2022. Along with paper and electronic invoices, structured invoices will be accepted forms of sales documentation. Following receipt of the European Commission's derogation decision, the Ministry of Finance intends to make the use of the KSEF mandatory in 2024. (Ministry of Finance 2022.)

The National System of e-Invoice (KSeF) allows for the creation and distribution of structured invoices. In the beginning, structured invoices will be used in business transactions just like paper invoices and electronic invoices do now. The structured invoice is in xml format, which matches the logical structure of the e-Invoice FA (1), which is published in the Central Repository of Specimen Electronic Documents on the ePUAP platform. A pilot program involving taxpayer participation was launched from October to December 2021. It is possible to continue using the offered KSeF test environment to adjust the IT systems. The KSeF Test

Zone tab contains information about testing. The National System of e-Invoices was implemented as an optional solution on January 1, 2022. From that point on, the National System of e-Invoices (KSeF) can be used to send out structured invoices. The European Union Council decided that Poland will have to use electronic billing starting on January 1, 2024. The purpose of implementing the National System of e-Invoices, according to the justification of the draft act implementing the KSeF, is to strengthen the tax system, reduce irregularities in VAT settlement, and improve taxpayers' conditions for conducting business activity through easier and faster access to documents. At the same time, this strategy is intended to counteract abusive taxpayer behaviors. The KSEF will help to increase the control of the correctness of tax settlements on goods and services while also simplifying the process of managing settlements with entrepreneurs. The amendment's solutions are also intended to generate more revenue for the state budget by making it easier to collect VAT at every stage of the transaction of goods and services. (Ministry of Finance 2022; Chyra & Dziwińska 2022.)

Receiving structured invoices will demand approval from the recipient. The consent should be granted under the same conditions as for electronic invoices. For receiving structured bills, the FSC will not handle the receiver approval process. If the recipient does not agree to receive it, the issuer retains the authority to issue a structured invoice in the system, and the invoice created in this manner can be passed to the recipient in another agreed-upon manner, such as through e-mail (such a document will retain the value of a structured invoice, which will meet the statutory conditions). The invoice identification number will be of a systemic type and should not be confused with the number mentioned in VAT Act 106e/2004. The day an invoice structured by the system is assigned a number identifying that invoice, it is issued and received at the same time. To change a structured invoice, it is needed to send a new invoice through KSeF. The elimination of the necessity to produce invoices issued in the KSeF system as part of the JPK file for invoices (JPK FA) at the request of the tax authorities is one of the benefits of developments in e-invoicing in Poland. The waiting period for a VAT refund has also been reduced from 60 to 40 days. (VAT Act 106e/2004; Chyra & Dziwińska 2022.)

3 Methodology

This thesis was written in the style of qualitative research. The research began with a review of the literature on data protection laws in Poland and Pagero's approach to them. The first section contains general information about the topic of the thesis, such as laws, directives, acts, and professional and organizational materials. The first step was to conduct research using a narrative overview, also known as a descriptive literature review. Data security is a broad topic. The best way to investigate it was to conduct a literature review. This was because the majority of the information was in Polish and there were many materials to

study. The purpose of the second phase was to give a company's perspective on the findings of the descriptive literature review.

For the second phase, the concept interview was chosen as the research method. The interviews were held to augment the findings of the literature review with experience-based expert knowledge and to establish how far the findings of the literature study might be used at Pagero. The goal was to evaluate these research methodologies and then seek content similarities and differences.

3.1 Literature review

The process of reviewing literature clarifies and defines terminology and essential topics in the context of the thesis. It enables us to put the topic within the historical context. It helps in the establishment of the theoretical framework that shapes the process. A literature review investigates scientific literature on a certain issue. Examines, assesses, and synthesizes relevant experts' research findings, theories, and practices. The author should present an in-depth, analytical, and reliable review of current knowledge, compare scientific works and theories, identify gaps in the literature, and provide solutions to the chosen subject. A literature review can be done on its own or as part of a broader study. The incorporated literature review, which provides context for the investigation, is more common. This sort of evaluation relates the sources to the subject of the study and influences the study's future design. The author demonstrates how the proposed study might boost knowledge and comprehension in the field. This evaluation of literature serves as the foundation for theses, dissertations, research initiatives, and fundings. Literature reviews, both independent and integrated, demonstrate how knowledge grows and accumulates. (Efron & Ravid 2018.)

Many different types of literature reviews have arisen over the years, but the four basic categories are traditional or narrative, systematic, meta-analysis, and meta-synthesis. A traditional or narrative literature review's primary goal is to examine and summarize a body of literature. This is accomplished by offering a full history of the literature on the relevant topic to highlight new research streams, uncover gaps, or detect contradictions. This form of literature evaluation can aid in the refinement, focus, and framing of research topics, as well as the development of theoretical and conceptual frameworks. A systematic literature review takes a more thorough approach to reviewing the literature, maybe because this sort of study is frequently employed to answer highly structured and detailed research objectives. The meta-analysis literature review entails extracting findings from the selected literature and assessing them using established statistical methodologies. Some argue that meta-analysis approaches aid in reaching conclusions, identifying patterns and correlations among findings. Meta-synthesis, which is a non-statistical method that assesses and analyzes qualitative study

findings. Including seeking to build on earlier conceptualizations and interpretations. (O'Gorman & MacIntosh 2015.)

Because it is a scholarly article that provides an overview of current understanding on a topic, a narrative literature review was chosen for this thesis. According to a traditional- narrative - review, the research topic should be limited while remaining broad enough to accommodate several research approaches and procedures. The emphasis is mostly on qualitative and mixed-methods research. Consider the ideas, concepts, or issues in your topic, the essential variables, and the point of view you wish to emphasize. As the literature review process progresses, it is normal for the primary research topic to evolve and be improved. (Efron & Ravid 2018.)

3.1.1 Database and selection of the material

During the assessment of the relevant content, both Google Advanced Search and ProQuest Central were employed. By using Google Advanced Search functions, there is less chance of finding irrelevant results. It frequently displays relevant information that may be unavailable during basic Google searches. It has been crucial while searching for data protection information in Poland, electronic invoicing, or the most up-to-date news about the Polish mandate regarding e-invoicing.

ProQuest Central, due to its big data base will ensure that the materials are useful and will help in selecting the best approaches to handle this problem. In the search, the following phrases were used: "Data Protection," "Electronic invoicing," "E-invoicing in Poland," and "KSeF." Advanced search and logic operators were employed in the databases whenever possible. When it comes to inclusion and exclusion criteria, the databases used a variety of restriction options. This contributed to the search results being more relevant to the requirements.

The search material was derived from scientific publications and books, as well as government authorities. Research was made in English and Polish, and the selected materials have been published since 2004. Based on the exclusion criteria (study was published in a language other than English or Polish, study was published before 2004), a significant amount of information was already removed from the search results based solely on the title. The titles of the items chosen for additional review were read, and their content was compared to the study's question.

3.1.2 Analysis of the literature review

The majority of the resources were in the English language. It is indeed possible that this is because electronic invoicing and other similar concepts are still relatively new in Poland.

However, because of the recent legislation enacted in Poland requiring all businesses to use electronic invoices, there were a great number of abstracts and articles provided by businesses in Poland as well as the country's Ministry of Finance.

Most of the legislation related to data security and data privacy was available in both English and Polish. Since they were standardized by the nations that constitute the European Union and its members. It was critical to place a strong emphasis on sourcing materials with a connection to Poland, as well as determining what kinds of rules and regulations exist in that country regarding the protection of personal information in electronic invoicing.

The information chosen for examination has been grouped into themes. The most general information regarding the subject of the thesis, which are: data protection, security protection and electronic invoicing. The second one is about the relevant legislations and laws in Poland. The third one is about Pagero and its entrance in the Polish market. During the data security and data protection research, the following terms were used: General Data Protection Regulation, ISO/IEC 27001:2013, ISAE3000 SOC2 Type, and Polish Telecommunication Act. The other topic of discussion was electronic invoicing in Poland. To better explain this section, it was required to first discover what electronic invoicing is and how it developed. It was also critical to explain the situation with electronic invoicing in Poland, the new e-invoicing regulation (KSeF), and how Pagero is compliant with the data protection in Polish market.

3.2 Interview

In qualitative research, one method known as an interview is used to collect data by questions asked of the participant. In an interview, there are at least two people, one of whom is designated as the interviewer and overseas asking the questions. There are many distinct kinds of interviews, which are typically distinguished from one another based on the amount of structure they possess. The first one is structured interview. This one is used in surveys and is often based on the same research reasoning as questionnaires: standardized ways of asking questions are considered to lead to answers that can be compared and possibly quantified across participants. Although planned interviews are effective for some purposes, they fail to capitalize on the dialogical potential for knowledge production that exists in human conversations. They are passive records of people's thoughts and attitudes, and they frequently disclose more about cultural norms about how to respond to certain inquiries than about the conversational production of social life itself. (Brinkmann 2013.)

The second is an unstructured interview. It is dedicated to an individual can only be determined by spending time with the interviewee, which implies that the interviewer cannot prepare for a life story interview by developing a long list of questions but must instead consider how to assist the telling of the life story. Following the initial request for a

narrative, the interviewer's primary responsibility is to listen, resisting the impulse to interrupt and occasionally asking clarifying questions. This does not have to be about the life story, but about other, more specific, storied parts of human existence, based on the narratological insight that humans experience and behave in the world through narratives. In this context, narratives serve as a root metaphor for psychological processes. (Brinkmann 2013.)

And the third interview is semi-structed. Semi-structured interviews are occasionally confused with qualitative interviews as such. They are most likely the most common in the human and social sciences and are sometimes the sole format addressed in texts on qualitative research. Semi-structured interviews, as opposed to structured interviews, can make better use of the knowledge-producing potential of dialogues by leaving considerably more discretion for following up on whatever aspects the interviewee deems important. Semi-structured interviews also allow the interviewer to become visible as a knowledge-producing participant in the process rather than hiding behind a pre-written interview guide. In addition, unlike unstructured interviews, the interviewer has greater control over how the conversation is oriented toward themes relevant to the study project. (Brinkmann 2013.)

A semi-structured interview was selected as a method since from the point of view of the topic of the thesis certain recurring features could be observed in the literature. The questions were formulated with a fixed set of open-ended questions, where the participants were invited to respond in their own words. This kind of interview gives a possibility for discussion and complex answers. Writing the knowledge base of the thesis and getting to know the topic more widely helped to prepare interview questions in such a way that it would be possible to find out possible challenges of the data protection for e-invoicing in Poland in Pagero's case.

I asked for an interview with one person whose main responsibility at work is data protection. This made sense because the Data Protection Officer would have the most data protection knowledge and experience. Especially for the purposes of the research, I wanted to ask specific questions about a particular market, which in this case was Poland.

Due to logistical limitations, the interview was conducted online. The identical questions were asked of each participant to check if their replies differed noticeably. Questions were prepared beforehand, and notes were taken during the meeting.

The major goal of the interview was to learn how Pagero is prepared for Polish customers in terms of data protection in e-invoicing. I chose the DPO for an interview because I wanted to analyze the subject as comprehensively as I could. It was necessary to find a knowledgeable individual who is the most familiar with the subject. DPO was also able to establish a common set of takeaways and ensure that no highly classified information was shared thanks to their

experience and practice in the field due to security reasons. The interview consists of several questions (Appendix 1).

3.2.1 Interviewee

For the purpose of this thesis, I made the decision to conduct an interview with the employee of the organization who possesses the greatest amount of knowledge and experience concerning data protection. I began by sending an email to the Data Protection Officer (DPO), providing information about my thesis and the possibility of attempting to set up an interview. Following the scheduling of an appointment, the discussion with the Data Protection Officer took place via Microsoft Teams. I came up with semi-structured questions (Appendix 1) so as to direct the conversation while at the same time giving the person being interviewed the opportunity to give open responses. During the interview notes has been taken for further data analysis.

The primary obligation of the Data Protection Officer is to exercise governance over data protection. In addition, in accordance with the description of the GDPR, it is to ensure that a company complies with all applicable data protection laws when processing the personal data of its employees, customers, suppliers, or any other people. This applies to any and all processing of personal data. In addition, it helps organizations through coaching, training, and raising awareness.

The purpose of the interview was to gather information from data protection industry professionals about their perspectives on the importance of data security in e-invoicing and how Pagero intends to conduct business in the Polish market. Once again, the interview and research materials were used to help address the thesis question regarding the compliance of Pagero's services with data protection for e-invoicing in Poland. The question was posed by the author of the thesis.

To the question, “What are the main challenges in data protection for e-invoicing?” The answer was that: “The biggest problem is that customers do not know exactly what Pagero does. When it comes to choosing Pagero as your service provider, customers do not think we have insufficient key management; rather, they prefer to be able to bring their own encryption keys, which is unfortunately not possible because part of our service is to format and encrypt the data, which is impossible to accomplish if it is encrypted.”

The second question was about: "What kinds of complaints about data protection customers have been made most commonly?"- “The most prevalent protection issues are those generated by inadequate key management because it may result in a data breach or loss.”

“What steps have been taken to comply with Polish law regarding data privacy and security?” – “Pagero has examined what laws apply in the European Union, as Poland is a member state, to ensure compliance with Polish privacy law.”

“How is Pagero up to date with Poland's data protection requirements?” – “Pagero continuously observes the markets in which it operates and modifies them as necessary.”

“What advantages in data security do Pagero's services have over its competitors in the Polish market?” – the answer to this question was that “The number of certificates company possesses in the field of data protection and security.”

3.2.2 Analysis of the interview material

As mentioned in the previous paragraph, the Data Protection Officer is mainly responsible for monitoring and driving processes of data protection in addition to role description in GDPR. “The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner in all issues which relate to the protection of personal data” (Article 38 of GDPR), which establishes the position of the DPO. Article 38 of GDPR specifies that other employees within the organization are prohibited from providing the DPO with instructions regarding the performance of their duties. Not only does the DPO have extensive responsibilities, but the position is also shielded from potential organizational interference. Overall, the DPO must keep their actions secret and will only report directly to the organization's highest level of management. (GDPR 2022.)

After the interview, the notes that were taken during the interview were written down for analysis. It helped to familiarize better with gathered data. As a next step, I went through the responses and attempted to categorize them according to the themes. The best approach to do so was to see which questions addressed comparable issues. This is why I wrote everything down and tried to mark the shared contents. I concluded that the first is generic data protection information. Questions three and four, which are relevant to the Polish market and how data protection is handled there, as well as Pagero's approach to it. Questions two and five are more specific to Pagero because they include the benefits and drawbacks of services. The second question is about information regarding common complaints, and in the fifth, what are the advantages over competitors. At the same time, Pagero's commitment to educating its personnel on the importance of data security and privacy was stated clearly during the interview.

4 Results

In this thesis, two methods were employed: a literature review and a supplementary semi-structured interview. Several themes emerged from the examination of both techniques. The themes were quite comparable in both cases. In this chapter, I will compare the outcomes of the two methods. The analysis of observations found in the previous research, followed by the findings of the interviews that were carried out, will each have its own set of results that will be presented below. All EU members are governed by the first three laws, which exist generally as EU regulations. The fourth one, on the Telecommunications Act, is specific to the Polish market. These aspects are presented as an answer for the research question. Based on the data found through literature review and interview presents that Pagero is compliant with data protection requirements in Poland.

The GDPR is the most important rule about protecting data in Poland. It is a set of laws that teach businesses and customers about their rights and responsibilities when it comes to personal information. Choosing a Data Protection Officer (DPO) is one of the most important and basic tasks for organizations where data processing is a key part of doing business. Also, if there was a data leak that could have led to sensitive information getting out, the GDPR says that the person in charge of the data must tell the person affected within 72 hours. The other requirement is to keep a record of what kinds of data are processed, why they are processed, how they are processed, and who is responsible for processing them. This is true for any use of personal information. (Pilarski 2019)

The General Data Protection Regulation is not the only standard that can be used. ISO/IEC 27001:2013 and ISAE 3000 SOC 2 Type 2 are two other examples. Both ISAE 3000 SOC 2 Type 2 and ISO/IEC 27001 talk about many of the same things. The security controls in both standards include procedures, guidelines, and tools that are meant to keep private data safe. Organizations only must adopt a control from the ISO/IEC 27001 standard or the ISAE 3000 SOC 2 Type 2 framework if that control is relevant to the organization's risk profile. ISO/IEC 27001 is built around an ISMS (information security management system), which is a way to manage data protection policies. To make sure compliance, risks must be evaluated, security controls must be chosen and put in place, and the results of these steps must be checked on a regular basis. But ISAE 3000 SOC 2 Type 2 gives even more room for error. It has five Trust Services Principles, but only the first one, “security,” is required. The other four—processing integrity, confidentiality, privacy, and availability—are optional. An organization doesn't have to set up internal controls for the other principles to get certified but doing so can help the organization meet the standards. (Irwin 2022)

The Telecommunications Law in Poland covers marketing calls and the transfer of marketing information through telecommunications terminal equipment. This includes SMS/MMS, email, and phone calls, including those from telemarketers. This means that if a business owner wants to call a customer with a marketing offer, they have to get their permission first. It is against the law to call, email, or text a subscriber without their permission. The Telecommunications Law limits entrepreneurs' rights to do telemarketing and e-marketing in a big way through its provisions. This includes SMS/MMS, email, and phone calls, including those from telemarketers. This means that if a business owner wants to call a customer with a marketing offer, they must get their permission first. It is against the law to call, email, or text a subscriber without their permission. The Act's rules make it much harder for entrepreneurs to use telemarketing and online marketing. GDPR and Poland's Telecommunications Act have similar rules about how to protect personal information. (Kowalczuk-Pakula, Jaraczewska & Stępień 2022.)

In the end, a theme will be talked about Pagero and why it went into the Polish market. Pagero is a service that helps businesses connect with each other and set up networks that make it easy for business documents like invoices, purchase orders, and other financial transactions to be sent and received digitally and automatically. This can be used by any business, no matter what industry it is in. Pagero checks to make sure that their products follow the rules of each country. The law says that all Polish businesses will have to send invoices electronically starting in 2024. All taxpayers must send and receive invoices through the National System of e-Invoices (Krajowy System e-Faktur). Pagero has a good chance of getting more customers in Poland because it is a multinational company. Pagero follows General Data Protection Regulation (GDPR) requirements for data security and holds other relevant certifications, such as ISO/IEC 27001:2013 or ISAE 3000 SOC 2 Type 2, which are also required in Poland. (Pagero 2022.)

Now, I'll talk about the themes that came up during the analysis and present the results of the interviews. The interview's main point about data protection is that it's important to point out that customers don't know how Pagero's services work, which is the biggest problem in the industry when it comes to electronic invoicing. People often say that electronic invoicing is new for many businesses and that they are moving a little too quickly with it. Most people know that when it comes to electronic invoicing, customers are in a hurry. They want a solution right away, but most of the time they don't care about keeping the information safe.

The next thing to talk about is how Pagero plans to do business in Poland. During the interview, it was said that Pagero meets the Polish rules for protecting personal information. This is mostly based on what people generally know about data protection in the EU, of which Poland is a member. In other words, figuring out where a new market is the first step in

getting into it. In the case of Poland, it has been treated the same as other markets in the EU.

Another point of disagreement is Pagero's competitive advantage on the Polish market, as well as the most common data protection complaints that were brought up during the interview. Pagero has a much larger number of certificates for data protection and security than other service providers. Customers do not think we have insufficient key management; rather, they prefer to be able to bring their own encryption keys, which is unfortunately not possible because part of our service is to format and encrypt the data, which is impossible to accomplish if it is encrypted.

In addition to getting the necessary certificates, the company's plan is to raise awareness about data protection throughout the organization. Once per year, all employees must take mandatory courses again through a learning platform to update their knowledge (such as the incident process).

5 Conclusion

Data protection is of the utmost importance for all documents, including electronic invoices. Threats to businesses and other types of entities are plentiful. Businesses must have a comprehensive understanding of how to protect not only their own but also their customers' data. By passing state-level laws and regulations, the use of paper is made more secure.

The goal of this research is to verify whether Pagero, a Polish service provider, complies with local data protection rules in e-invoicing. Based on the information gathered from the literature review and interview, it is easy to conclude that Pagero has been well-organized in terms of data protection not only for the Polish market but also for the global market by answering the research question, "How are Pagero's services compliant with Polish law and regulations regarding data protection for e-invoicing?" Pagero has been on the market for around 20 years and is well-known in the Nordic advanced electronic invoicing sector. Pagero tracks and updates legal and legislative changes, particularly in the European Union. The General Data Protection Regulation is Pagero's primary data protection statute.

Pagero is accountable for complying with GDPR rules. The data protection policy's objective is to assist Pagero and its customers in meeting compliance requirements and other data protection requirements linked with the use of Pagero's services. To be relevant, the management system must be regularly adjusted and developed in response to changing business needs.

Overall, Pagero is constantly developing risk and incident management methods. Policies, guidelines, process descriptions, instructions, and security awareness training guarantee that Pagero employees understand how to securely handle client data and respond to an incident. Customers will undoubtedly profit from using Pagero's services because they are in accordance with Polish data protection rules. The business monitors the marketplaces to verify that they are legitimately certified. One possibility for the company on how to use this thesis is to publish a booklet regarding data protection in Poland for sales or commercial purposes.

References

Printed

Calder, A. 2017. EU General Data Protection Regulation (GDPR)An implementation and compliance guide. Second edition. IT Governance Privacy Team. IT Governance Publishing

O'Gorman, K., MacIntosh, R. 2015. Research methods for business & management: a guide to writing your dissertation. Chapter 3 The Literature Review / O'Gorman and MacIntosh. 2nd edition. Goodfellow Publishers Ltd 2015

Electronic

Anton, I. 2022. SOC2 (ISAE3000) certification. Accessed 24 September 2022. https://home.kpmg/ee/en/home/services/management-and-risk-consulting/soc2--isae3000--certification.html

Brinkmann, S. 2013. Qualitative interviewing. Accessed 10 October 2022. https://ebookcentral.proquest.com/lib/laurea/reader.action?docID=1274289&ppg=174#

Buttarelli, G. 2013. European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the Commission Proposal for a Directive of the European Parliament and the Council on electronic invoicing in public procurement. Accessed 27 September 2022. https://edps.europa.eu/sites/edp/files/publication/13-11-11_electronic_invoicing_en.pdf

Calder, A. 2018. EU GDPR – a Pocket Guide, Second Edition. Accessed 3 October 2022. https://ebookcentral.proquest.com/lib/laurea/reader.action?docID=5796949

Chyra, S. Dziwińska K. 2022. Krajowy System e-Faktur – założenia i potencjalne korzyści. Accessed 20 September 2022. https://firma.rp.pl/ksiegowosc/art35655931-krajowy-system-e-faktur-zalozenia-i-potencjalne-korzysci

DataGuard. 2022. SOC 2 vs ISO/IEC 27001: Key Differences Explained. Accessed 20 September 2022. https://www.dataguard.co.uk/blog/soc-2-vs-iso-27001/

Data Interchange. 2022. What is EDI: The History and Future of Electronic Data Interchange. Accessed 10 September 2022. https://datainterchange.com/what-is-edi/

Digital Sense. 2022. To Protect or Secure: That Is the Question. Data Protection vs Data Security. Accessed 29 September 2022. http://digitalsense.com.au/to-protect-or-secure-that-is-the-question/

Directive 2014/55/EU. European Parliament and of the Council on electronic invoicing in public procurement Text with EEA relevance. Official Journal of the European Union.

26.05.2014. Accessed 28 September 2022. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32014L0055

Efron, S.E., Ravid R. 2018. Writing the Literature Review: A Practical Guide. Accessed 5 October 2022. https://ebookcentral.proquest.com/lib/laurea/reader.action?docID=5522670

E-InvoicingBasics. 2022. Types of eInvoicing. Accessed 28 September 2022. https://www.einvoicingbasics.co.uk/what-is-e-invoicing/types-of-einvoice/

Endresen, L. 2021. Sustainable business: E-invoicing, your company and the environment. Pagero. Accessed 20 September 2022. https://www.pagero.com/blog/sustainable-business/

European Commission. 2022. Types of digital invoices. Accessed 21 August. 2022. https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Types+of+digital+invoices#Typesofdigitalinvoices-1

European Commission. 2022. What is eInvoicing. Accessed 21 August. 2022. https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/What+is+eInvoicing

European Union. 2022. Data Protection under GDPR. Accessed 25 July 2022. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

European Union law. 2016. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance). Accessed 10 July 2022. https://eur-lex.europa.eu/eli/dir/2016/943/oj?locale=en

General Data Protection Regulation. 2016. Accessed 22 July 2022. https://gdpr-info.eu/

IBM. 2022. Why is data security important? Accessed 19 September 2022. https://www.ibm.com/se-en/topics/data-security

ISO/IEC 27001:2013(en) Information technology. Security techniques. Information security management systems. Requirements. Accessed 22 July 2022. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO/IEC 27001:2022(en) — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Accessed 11 December 2022. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en

Irwin, L. 2022. ISO/IEC 27001 vs SOC 2 Certification: What's the Difference? IT governance. Accessed 28 November 2022. https://www.itgovernance.eu/blog/en/iso-27001-vs-soc-2-certification-whats-the-difference

Kowalczuk-Pakula, I. Jaraczewska, P. Stępień, E. 2022. Poland - Data Protection Overview. Accessed 12 September 2022. https://www.dataguidance.com/notes/poland-data-protection-overview#:~:text=The%20UODO%20is%20the%20main,the%20Office%20of%20Electronic%20Communications.

LeadDesk. 2021. What is ISAE 3000 SOC 2 and why is it important. Accessed 1 September 2022. https://leaddesk.com/blog/what-is-isae3000-soc-2-why-is-it-important/

McCarthy, B. 2013. The Logicbroker Blog. EDI History. Accessed 12 September 2022. https://blog.logicbroker.com/blog/2013/08/19/edi-history

Medius. 2022. What is e-Invoicing? The benefits of e-invoicing. Accessed 21 August 2022. https://www.medius.com/glossary/what-is-e-invoicing/

Ministry of Finance in Poland. 2022. Informacje o KSeF. Accessed 1 October. 2022. https://www.podatki.gov.pl/ksef/informacje-o-ksef/

Ministry of Finance in Poland. 2022. National e-Invoicing System. Accessed 25 September 2022. https://www.gov.pl/web/finanse/ue-zgadza-sie-na-obowiazkowa-e-fakture-w-polsce-od-2024-r

Moran, M. 2022. What is an e-invoice? Pagero. Accessed 28 November 2022. https://www.pagero.com/blog/what-is-an-e-invoice-blog/

Pagero. 2022. Information security. Accessed 29 August 2022. https://www.pagero.com/information-security/

Pagero. 2021. Annual Report 2021. Accessed 26 July 2022. https://www.pagero.com/downloads/documents/Annual_Report_2021_eng.pdf

Pagero. 2022. Electronic Data Interchange (EDI) 2.0. Accessed 2 September 2022. https://www.pagero.com/solutions/edi/

Pilarski, R. 2019.Poradnik Przedsiębiorcy. RODO dla przedsiębiorcy w jednoosobowej firmie. Accessed 28 September 2022. https://poradnikprzedsiebiorcy.pl/-rodo-dla-przedsiebiorcy-w-jednoosobowej-firmie

Posey, B. 2021. TechTarget. Comparing data protection vs. data security vs. data privacy. Accessed 29 September 2022. https://www.techtarget.com/searchdatabackup/tip/Comparing-data-protection-vs-data-security-vs-data-privacy

Prawo telekomunikacyjne. 2022. Accessed 2 September 2022. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20041711800/U/D20041800Lj.pdf

Soc2.co.uk. 2022. SOC 2 & ISAE 3000. Accessed 1 September 2022. https://soc2.co.uk/soc-2#:~:text=ISAE%203000%20is%20the%20international,based%20on%20Trust%20Services%20Criteria

Tarnobrzeska, P. 2019. Prawo telekomunikacyjne w firmie – prawa i obowiązki przedsiębiorców. Accessed 2 September 2022. https://informaticalegis.com/prawo-telekomunikacyjne-w-firmie-prawa-i-obowiazki-przedsiebiorcow/

UODO. 2019. Ustawa z 10 maja 2018 o ochronie danych Osobowych. Accessed 2 September 2022. https://uodo.gov.pl/pl/395/1192

Wolford, B. 2022. What is GDPR, the EU's new data protection law? Accessed 29 September 2022. https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

VAT Act 106e/2004. Accessed 24 September 2022. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20040540535/U/D20040535Lj.pdf

Zavorskas, W. 2020. LinkedIn. A history of EDI. Accessed 10 September 2022. https://www.linkedin.com/pulse/history-edi-william-zavorskas/

Figures

Figure 1. COSO's 17 Principles of Internal Control (LeadDesk 2022)..... 11

Tables

Table 1. Differences between SOC 2 vs. ISO/IEC 27001 (DataGuard 2022)..... 12
Table 2. Types of digital invoice (European Commission 2022)..... 16

Appendices

Appendix 1: Questions for an interview 35

Appendix 1: Questions for an interview

1. What are the main challenges in data protection for e-invoicing?
2. What kind of complaints about data protection customers have been made the most commonly?
3. What steps have been taken to comply with Polish law data privacy and security?
4. How is Pagero up to date with Poland's data protection requirements?
5. What advantages in data security do Pagero's services have over its competitors in the Polish market?