



Международно Висше Бизнес Училище
International Business School

**SPECIFIC FEATURES OF THE APPLICATION OF THE
PERSONAL DATA PROTECTION REGIME IN
ACCORDANCE WITH THE GENERAL DATA
PROTECTION REGULATION IN ACCOUNTING**

ABSTRACT OF THE DISSERTATION

by Milena Svetlomirova Mitkova

For the award of the educational and scientific degree of Doctor in
Economics and Management (Industry) in professional field 3.8. Economics

Scientific supervisors:

Assoc. Prof. Dr. Daniela Ventsislavova Georgieva

Prof. Dr. Irina Tsakova

SOFIA

2025

The dissertation consists of 240 pages, including: title page, table of contents, list of abbreviations, list of graphs, tables, and figures, and dedication. The content includes an introduction (7 pages), main text (three chapters -140 pages), and conclusion (8 pages). The bibliography, 21 pages in length, is prepared in accordance with Bulgarian Standard BDS 690:2021 and includes 169 literary, normative, and online sources: 91 in English, 2 in German, 1 in Turkish, 2 in Spanish, 1 in Dutch, 2 in Italian, 2 in French, 1 in Polish, 1 in Swedish, and 66 in Bulgarian.

The dissertation also has 5 appendices – 52 pages. The main text of the dissertation includes 23 tables and 20 figures.

The author of the dissertation is a doctoral student in independent study at the International Business School – Botevgrad.

I. General characteristics of the dissertation

1. Relevance of the research

The development of information and communication technologies has led to the emergence of new digital tools for the collection, processing, and storage of personal data and digital transformation in all aspects of business relations at the national and international levels. These trends have resulted in risks to the security and privacy of personal information and potential damage from fraud, abuse, and the obstruction of individuals' rights (Datenschutzkonferenz (DSK), 2018). As a result, numerous international acts have been created to regulate and prevent the negative consequences of unlawful and unregulated access to personal information. For this reason, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) was adopted at the European level. The regulation considers the impact of technological progress and globalization¹. Accountants from specialized accounting firms² process various types and categories of personal data using specific digital tools and technologies to carry out their activities. A potential security breach could damage the organization's reputation but also lead to sanctions and penalties with serious

¹ "Globalization" is understood as "the integration of markets, nation states, and technologies ... in a way that allows individuals, corporations, and nation states to reach further, faster, deeper, and cheaper than ever before," according to Friedman (2012: 7–8).

² For the purposes of this dissertation and within the scope of the theoretical and empirical research, "specialized accounting firms" refers to any entity registered under the Commercial Law (CL) whose scope of activity includes organizing accounting and preparing financial statements, in accordance with paragraph 1, point 27 of the Additional Provisions of the Accounting Act.

economic consequences³. The implementation of new accounting software solutions for data collection, processing, and storage creates risks for information security. This is because systems are vulnerable to cyberattacks and unauthorized access, which can compromise stored financial information and personal data. In addition, the failure of accountants to identify and distinguish between possible risks and their impact on personal information results in a lack of sufficiently appropriate technical and organizational measures. This determines **the relevance** of the topic of the specific features of the application of the personal data protection regime in accounting.

2. Objectives and tasks of the dissertation

The aim of the study is *a theoretical and practical study and analysis of the specific features of the application of the personal data protection regime under the General Regulation in accounting, with a focus on the impact of digitization in specialized enterprises in Bulgaria.*

To achieve this goal, **the following research tasks** have been identified in this dissertation:

- to identify the priority digital technologies used in accounting to outline the main advantages, disadvantages, and risks to the security of personal information⁴ from digitization in accounting;

³ In 2019, there was "unauthorized access to about 3% of the information contained in the databases of the National Revenue Agency" (Commission for Personal Data Protection (CPDP) 2022).

⁴ For the purposes of this dissertation, "data" and "information," as well as "personal data," "personal information," and "individual information" are used synonymously and unambiguously, although the differences in the concepts are considered. The basis for such identification of meanings is the interpretation of the Article 29 Working Party on the application of the General Data Protection Regulation, where "data" is defined as "any information" relating to a natural person.

- to clarify the essence and meaning of the term "personal data" to more clearly define the information to be collected, stored, processed, and protected by accountants in Bulgaria;

- to examine the emergence and development of personal information protection legislation in Europe and Bulgaria and possible obstacles to compliance with the regulatory framework by specialized enterprises at the national level;

- to distinguish between accounting activities in specialized companies⁵ based on transactions and events with parties internal and external to the reporting entity. Of all external parties, a more in-depth analysis is carried out on relations with customers, suppliers, and certain other counterparties⁶ . From the group of internal parties, the subject of analysis is the staff of the enterprises;

- to study appropriate practices regarding personal information security measures relevant to the accounting sector and to provide guidelines for the creation of a Code of Conduct that considers the specificities of personal data processing in accounting.

3. Subject and object of the dissertation research

The object of the study is the specific features of accounting activities in specialized accounting enterprises in their capacity as data controllers.

The subject of the study is the currently applicable practices and procedures in accounting activities that are directly related to the collection,

⁵ In the context of the dissertation, the term "company" is used in the sense of a legal entity composed of two or more persons united for the purpose of conducting commercial activities with joint funds, in accordance with Article 63 of the Commercial Law. The terms "company" and "enterprise" are used synonymously, insofar as both refer to entities with legal personality under the applicable commercial law.

⁶ "Counterparty" means "a person or institution that assumes certain obligations under a contract, a party to a contract" from the Bulgarian Language Dictionary (1993).

storage, and processing of personal data of third parties. In addition, the main sources and technical means for collecting and processing personal information by type are examined, based on whether the persons are internal or external to the reporting entity.

4. Research thesis and author's hypotheses

The thesis of the study is that digitization in accounting activities poses risks in the processing of personal data, which require a systematic analysis of the legal framework and the principle of accountability with a view to developing effective practices for information protection.

The dissertation research puts forward several working **hypotheses**, namely:

- the digitization and use of new technological software solutions in accounting create risks to the security and confidentiality of personal information;
- the identification and assessment of the risks of personal data processing when using innovations⁷ in accounting is a prerequisite for the selection of appropriate technical, organizational, documentary, and personal measures to protect the information of data subjects (e.g., encryption and others);
- the interpretation of the complex regulatory regime by accountants in accounting firms is difficult due to the lack of clear and specific guidelines for compliance with the regulatory framework and leading to violations of the principles and inconsistent application of the rules on information protection;

⁷ In this context, innovation is not used in the sense of a technology that is unique and produced/invented by the accountant, but rather software that has been created and exploited on a global scale, but which accountants in Bulgaria are implementing and using in their work for the first time.

- The introduction of certification training by accredited organizations to ensure that data protection officers acquire up-to-date and sufficient knowledge would better guarantee the performance of tasks to maintain an adequate level of protection and security by organizations.
- The development of and adherence to a Code of Conduct for the accounting sector would contribute to the fulfillment of obligations under personal data protection legislation, reflecting the specificities of the industry.
- The role of accounting firms in Bulgaria, as data protection officers, is essential for preventing financial and other abuses and imposing administrative fines on organizations and individual clients.

5. Research methodology

For the purposes of verifying the author's theses and hypotheses and preparing assessments, various **general scientific methods and approaches** were used, such as the comparative method, the method of analysis and synthesis, as well as historical, logical, complex, systematic, analogical, inductive, and deductive approaches. In order to achieve the research goals and objectives of the study, a theoretical study of information from publications by Bulgarian and foreign authors was conducted. The dissertation presents data from the author's questionnaire surveys and individual in-depth semi-structured interviews with practicing accountants. The aim is to conclude the performance of their duties in the field of personal data protection legislation and the digital technologies used in their work. Tables and figures are used to visualize the analyses and conclusions. Krammer's X (2) analysis of statistical relationships and dependencies is used to test the hypotheses.

6. Limitations of the study

The scientific development is limited to the analysis of certain specific features of accounting activities that are directly related to the collection, storage, and processing of third-party personal data. In this sense, we can point out **the** following **limitations**:

- ***time limitation*** – the starting date for the dissertation research is October 2021 and is in line with the legislation in force as of February 2025;

- ***spatial and thematic limitation*** – despite the wide variety of publications, reports, and other scientific sources, it is not possible to cover all available information for review. The empirical data was collected from surveys and interviews with specific respondents from practicing accountants due to the impossibility of covering all subjects and all issues in accordance with personal data protection legislation;

- ***Information limitation*** – the data and literature used for the purposes of the analysis are public and freely accessible.

- ***Industry limitation*** – the reporting unit in the dissertation is accountants from specialized accounting firms in Bulgaria in their capacity as administrators and processors of personal data.

7. Approval

Part of the content of the dissertation research has been published (including studies, results, figures, tables, findings, and conclusions).

II. Structure and content of the dissertation

Contents

List of abbreviations used

List of graphs, tables, and figures used

Dedication

Introduction

I. CHAPTER ONE: Nature, significance, and regulatory framework of personal data protection

1. Impact of digitization and technological progress on accounting and data confidentiality

2. Essence and significance of the concept of "personal data"

2.1 Etymology and meaning of the concepts of "information" and "data"

2.2 Study of "personal data" by the scientific research community in the Bulgarian database "COBISS+"

2.3 Concepts for interpreting "personal data" in the context of EU data protection law

3. Regulatory framework in Europe and Bulgaria regarding personal data protection

II. CHAPTER TWO: Specific features of the procedures for compliance with the regulatory framework for personal data protection by accounting firms

1. Accounting firms as controllers and processors of personal data

2. Differentiation of activities in specialized accounting firms with regard to the regulatory framework for personal data protection.

2.1 Differentiation of the activities of accounting firms based on interaction and communication with clients for the purposes of personal data protection

2.2 Differentiation of activities in specialized accounting firms for the purposes of the regulatory framework for data protection based on

interaction and communication with suppliers and other counterparties (lenders and borrowers)

2.3 Differentiation of activities in specialized accounting firms for the purposes of data protection legislation with staff

2.4. Measures to protect information when processing personal data by specialized accounting firms

3. Functions and requirements for personal data protection officers in accounting firms

III. CHAPTER THREE: Study of the measures and procedures applied in accordance with the personal data protection regulations by specialized accounting firms in Bulgaria

1. Research methodology and author's hypotheses

2. Results of empirical studies

2.1. Analysis of the relationship between assessing and identifying the risks of processing personal information (including cyber risks) and the choice of specific measures and practices for personal data protection

2.2. Analysis of the relationship between the implementation of innovative digital tools for the collection, processing, and storage of data by specialized accounting firms and the increase in cyber risks to the confidentiality of information

2.3 . Investigation of opportunities for improving and maintaining a high level of competence and professional skills in personal data protection on the part of accountants

2.4 . Summary of the three empirical studies and discussion

3 Recommendations for the development of a Code of Conduct for the accounting sector in the context of personal data protection

Conclusion

List of references

Appendices

III. Summary of the dissertation

Introduction

The introduction justifies the relevance of the topic, its goals, and objectives. It defines the object, subject, main thesis defended by the author, and working hypotheses. It describes research methodology and the selected methods. It outlines the scope of the research and its significance.

CHAPTER ONE. Essence, significance, and regulatory framework of personal data protection

The first chapter of the dissertation examines specialized literary sources and presents the essence, significance, and development of the regulatory framework for personal data protection in Europe and Bulgaria, as well as its impact in an international context. Digital technologies used in accounting are also examined, specifically the risks they pose to the confidentiality and security of personal information. The general theory examines the works of various authors who explore the definition of the concept of "personal data," which form the basis for the subsequent analysis of the specifics of the procedures for compliance with the legislation by specialized accounting firms, in accordance with their inherent activities. Based on the etymology and meaning of the terms "information" and "data" and on concepts for interpreting "personal data" in the context of EU data protection law, a proposal is made for a definition of the two terms for accounting purposes.

Point 1: Impact of digitalization and technological progress on accounting and data confidentiality summarizes the reasons why European governments are proactive in promoting digitalization, business automation, modernization of public and administrative services, and improving the technological skills of the workforce. The main reasons for this are:

- economic competitiveness and growth: digitization attracts investment and encourages digital entrepreneurship;
- efficient public services and reduced bureaucracy;
- innovation and job creation: governments see digital technologies as a mechanism for generating research, new business opportunities, and employment.

Based on various literary sources, the advantages (Gonçalves et al. 2022; Lazarova 2020; Davern et al. 2019) of the technologies used in accounting, as well as some disadvantages (Boban & Stipić 2020; Davern et al. 2019)

Digitization and the use of new technologies in accounting increase efficiency, accuracy, and profitability. Despite the many benefits, there are risks to cybersecurity, which is a priority for accounting and business, as a breach in the security of accounting systems "could shut down an entire critical infrastructure industry and threaten organisational survival" (Gonçalves et al. 2022: 3) In addition, "unauthorized use of information generated in the accounting system can lead to detrimental consequences, risking loss of information, incorrect data entry and misuse of confidential information" (Lehenchuk et al. 2022: 40).

The dissertation presents some of the risks associated with the cybersecurity of information generated in electronic accounting systems:

- risks related to the collection and entry of data into an automated system – intentional or unintentional entry of incorrect or inaccurate data or its destruction;
- risks related to the processing and storage of data on electronic media – unauthorized access or deletion, destruction, or damage;
- risks related to the summarization and transfer of information – theft, misuse or redirection of data (Lehenchuk et al. 2022).

Limiting or eliminating information security risks is essential to minimize the potential negative consequences for both accounting firms and data subjects themselves. In view of the latter, it is necessary to prepare a risk assessment of data processing, as well as to implement internal control and

compliance with comprehensive measures, jointly by the management and the accounting department. The dissertation distinguishes three groups of measures:

- organizational – restricting access to confidential accounting information;
- technical – appropriate hardware and software;
- personnel – improving the competence of employees in the application of new information technologies (Lehenchuk et al. 2022).

Accounting, as an information and control system, is an indispensable part of the functioning of any enterprise. It provides information about the financial condition of the organization by processing and reporting data, which in some cases may be equivalent to personal data. A review of the specialized literature leads to the conclusion that the implementation of new accounting software solutions for data collection, processing, and storage creates risks for information security. These risks arise from the vulnerability of systems to cyberattacks and unauthorized access, which can compromise financial information and personal data. It is important to identify and assess the risks of using digital tools by accountants and the threats to the integrity, privacy, and confidentiality of data. Accountants from accounting firms in Bulgaria may not identify and distinguish the possible risks and their impact on personal information.

To mitigate risks to the security of personal information, accountants must correctly interpret and comply with data protection regulations. A thorough understanding of legal obligations and the implementation of appropriate technical and organizational measures to protect data is required. In this context, it is essential that accountants correctly understand the definition of "personal data" in order to comply with regulatory requirements in this area. For this reason, the next section of the dissertation examines the essence and meaning of the concept of "personal data."

In section 2, **"Essence and meaning of the concept of 'personal data' ,"** the definition of the concept in European law is examined, dividing it into its

constituent parts. It is concluded that no distinction is made between the terms "information" and "data," which suggests a broad interpretation of the term in terms of its nature, content, and form. In this context, it is considered appropriate and useful to clarify "information" and "data," which do not have uniformly accepted definitions and are analyzed in the context of different scientific fields.

In sub-section **2.1 Etymology and meaning of the terms "information" and "data,"** some of the various definitions of the concepts are examined, which facilitates a more detailed analysis of their meanings, and by accepting or rejecting one or another theoretical proposition, it is possible to distinguish between them in the context of personal data protection. The relationship between "information" and "data" is examined, and the definitions of Romney et al. (2017) of the concepts from an accounting perspective are presented.

At this stage, the author of the dissertation research concludes that it is not possible to unambiguously and in detail distinguish data from information based solely on etymological features and denotative meaning. A more in-depth analysis of their relationship and dependencies in the specific context of EU data protection law is needed, given that the lack of such interpretation and understanding may lead to errors in accounting theory and practice in the context of the correct determination of personal data subject to processing and storage. For accountants, clarifying the concept of "personal data" and the relationship between "data" and "information" is essential for the correct interpretation of information, facts, and circumstances in accordance with the law, ensuring secure and reliable processing of information, and effective management of the risk of security breaches.

Subsection **2.2 Study of "personal data" by the scientific research community in the Bulgarian database "COBISS+"** aims to examine the focus of academic research on the concept of "personal data" and to outline a current definition. It has been established that the concept of "personal data" has not been studied in sufficient depth. Based on the information set studied,

only a small part of the scientific research entered in the COBISS+ databases examines the essence of the definition of "personal data" laid down by the legislator. No resource offers a comprehensive analysis or examines and/or compares the term "information" with the term "data." The analyses are primarily from a legal perspective, with no economic analyses, which is an additional weakness of the scientific literature because it may lead to a misunderstanding of the essence of the concept by economists and, in particular, accountants. Internationally, the interpretation of the definition is accompanied by controversy and debate. Some researchers present up-to-date and in-depth studies that take into account, to the greatest extent possible, the relationship and dependencies between "data" and "information" in the context of EU data protection law. This requires a more in-depth study of European concepts and interpretations of the term "personal data." These studies are presented in subsection **2.3 Concepts for interpreting "personal data" in the context of EU data protection law.**

At this stage, the author of the dissertation concludes that Purtova (2018) and Gellert (2020) offer a contemporary and in-depth theoretical view of the definition of "personal data."

Purtova's (2018) conclusions are based on an analysis of the Article 29 Working Party Guidelines and the case law of the Court of Justice of the EU, with the author arguing that in the context of digital transformation, virtually any information can be linked to a specific natural person. According to this interpretation, the definition of personal data should be understood as broadly as possible, since any information has the potential to be linked to a specific person, either directly or through further processing. Even when data appears neutral or anonymous, it can become identifiable in a different context, with changes in technological capabilities, or through the use of external sources. In this way, the line between "identifiable" and "unidentifiable" content is becoming increasingly blurred.

Gellert (2020) analyzes the meaning of "data" and "information" by comparing the definitions in legislation and in information theory and

machine learning. In his study, the author argues that "in the legal definition of personal data, data is information. This is consistent with both a literal reading of the GDPR definition (Article 4.1 of the GDPR) and with "...a review of information theory."

The studies by Purtova (2018) and Gellert (2020) are the basis for the conclusion in the dissertation that in the context of data protection legislation, ***"data" and "information" are equivalent in meaning and can be used synonymously.*** Despite the above and based on the concept of Romney et al. (2017) for accounting purposes, it is proposed ***that "data" be understood as unstructured facts, a basic component of the accounting information system and accounting records of business transactions leading to a change in financial position. Information is a collection of organized, processed and structured data that has value, meaning and significance for management decision-making.*** In relation to legislation in the field of confidentiality, both the primary data itself and the information created on its basis are subject to protection, given that the data can generate information that relates to a specific natural person.

The following paragraphs provide a distinction between personal and non-personal data and summarize the legal grounds for the collection, processing, and storage of personal information. In this context, a distinction is made between personal information and methods by which data cannot be related to an identified natural person or a natural person who can be identified. Such techniques include anonymization, pseudonymization, and encryption.

The principles on the basis of which the processing of personal information is possible are systematized so that the rights of individuals are equal and protected. Given that proof of compliance with all principles is achieved through reporting, the author of the dissertation proposes that the principle of accountability should be the basis for the processing of personal data.

A historical review of the development of privacy regulations can clarify the natural logical connection between the need to preserve privacy and the legal means of data protection that accountants should apply. To this end, the following section examines European regulations and their implementation in Bulgaria.

Point 3. Regulatory framework in Europe and Bulgaria regarding personal data protection, based on "Handbook on European Data Protection Law" (European Union Agency for Fundamental Rights, 2018), presents in detail the evolution of European law in this area, describing the significant contributions and shortcomings of the main documents in the field of personal data protection. It points out that legislation in the field of personal data protection is in the process of being improved and that numerous gaps and shortcomings have been noted in the specialist literature. These include incomplete, inaccurate, or vague definitions of concepts (Thomson 1974), a lack of clear connection between the risks to privacy and their impact (Robinson et al. 2009), the creation of expanded powers for government agencies (Sloot 2014), and the presence of long and complex texts (Hoofnagle et al. 2019). These weaknesses in the regulatory framework are a prerequisite for possible difficulties in their interpretation by accountants for the lawful performance of their activities.

The dissertation study makes a comparative analysis of the regulatory framework in Europe and the US and concludes that the influence of the General Data Protection Regulation is growing, given the globalization of the economy and the possibility of movement of capital, people, and resources outside the borders of individual countries and continents. In support of this assertion, it is pointed out that legislative solutions regarding the protection of personal data are being created in other countries outside the European Union.

At this stage, the implementation of the regulation in our national legislation is being examined, and the conclusion is that the possibility of EU member states adopting alternative options, requirements, and conditions is a

prerequisite for the harmonization of control and enforcement of personal data protection in the European Union to be considered unfeasible.

In conclusion and summarizing the analyses in the Chapter, the regulation of personal data protection is inherently complex, voluminous, and in some cases unclear, but it contains principles that should be demonstrably complied with. Given that no clear and specific guidelines for compliance with the regulatory framework are provided, different interpretations and applications of the requirements are possible. Specialized accounting firms, in their capacity as administrators, are exposed to the risk of sanctions and damage to their prestige and reputation if non-compliance with the regulatory requirements is established. A critical component of legal compliance is identifying and assessing the potential risks associated with data processing activities and implementing measures to mitigate the impact of those risks. Effective risk management ensures that organizations can respond quickly and effectively to security incidents, minimizing potential damage. An appropriate and recommended approach to maintaining information security includes pseudonymization and encryption of personal data and/or regular testing and evaluation of the effectiveness of measures. Based on the analysis of the specialized literature, it is assumed that there may be a lack of understanding on the part of representatives and employees of specialized accounting firms regarding their specific obligations. For this reason, the following chapter examines the nature and characteristics of the procedures for compliance with the regulatory framework for the protection of personal data by accounting firms.

Chapter One addresses three of the research tasks presented in the introduction to the study:

- the digital technologies used as a priority in accounting activities are identified and the main advantages, disadvantages, and risks to the security of personal information from digitization in accounting are outlined;

- clarifies the essence and meaning of the term "personal data" in order to more clearly define the information to be collected, stored, processed, and protected by accountants in Bulgaria;

- examines the emergence and development of personal information protection legislation in Europe and Bulgaria and the possible obstacles to compliance with the regulatory framework by specialized companies in Bulgaria.

CHAPTER TWO. Specific features of the procedures for compliance with the regulatory framework for the protection of personal data by accounting firms

The second chapter presents a study of the specific features of the application of the personal data protection regime in accounting. The role of accountants as personal information administrators is examined in detail. The activities of specialized accounting firms are differentiated based on interaction and communication with external and internal counterparties in relation to data protection. Appropriate measures for the protection of information when processing personal data by specialized accounting firms and the functions and requirements for personal data protection officers in accounting firms have been examined.

In point **1. Accounting firms as controllers and processors of personal data**, the sources of personal data flow to accounting firms, the legal basis for their processing, and the possible categories and types of personal data are analyzed.

Personal information received by the company may be provided by external (customers, suppliers, public authorities, etc.) and internal sources (staff, owners, shareholders, etc.) electronically (website, e-mail, etc.), in person by the data subjects or by third parties to the company. Companies identify personal data flows and, if the information is not anonymous, the

accounting company collects and processes personal information only if there is a relevant legal basis and security and confidentiality measures are in place.

Accounting firms process personal data of people from within and outside the organization, as well as of counterparties, in compliance with the requirements of contract, labor, tax, health, social security, and other applicable legislation. Regulation (EU) 2016/679 does not provide specific criteria for systematizing information, so it is appropriate to classify data according to their characteristics and functions.

The Regulation requires controllers and processors of personal data to maintain records describing the categories of subjects and data processed. A clear distinction between accounting activities according to the transactions and events carried out, as well as the specification of the information processed, is a prerequisite for the fulfillment of regulatory obligations.

In point **2. Differentiation of activities in specialized accounting firms with regard to the regulatory framework for personal data protection** for the purposes of categorizing subjects and types of data subject to more in-depth analysis are accounting activities from the point of view of fulfilling obligations based on a contract with a client – client, contractual relationships with suppliers, certain counterparties, employment relationships based on the Labor Code and non-employment relationships based on the Law on Obligations and Contracts.

The contractual relationships arising between specialized accounting firms and their counterparties—including clients, suppliers, and other partners—go through several basic stages. These include: initiating pre-contractual communication, formalizing an agreement, fulfilling obligations, and subsequently terminating the established legal relationship.

Subsection **2.1 Distinguishing the activities of accounting firms based on interaction and communication with clients for the purposes of personal data protection** describes the stages of creation, implementation, and termination

of a contract for the provision of accounting services by specialized accounting firms and specifies their role as personal data controllers.

In the stages of creation, implementation, and termination of the contract for the provision of accounting services, specialized accounting firms usually act as personal data controllers and, in rarer cases, as processors for purposes and by means determined by the party assigning the processing task.

The contractual relationship between accounting firms and their clients goes through four main stages, which involve the processing of personal data.

The first stage (pre-contractual) aims to prepare a price offer and conclude a contract for the provision of services. In this process, personal information is collected and analyzed, the storage of which is regulated by the Anti-Money Laundering Act (AMLA) and the Anti-Terrorism Financing Act (ATFA). The regulatory framework defines the types of data, the storage periods (up to five years after the termination of the relationship), and the recipients, with the State Agency for National Security (SANS) as the main authority.

The second stage – the conclusion of a contract for the processing of personal data – is documented in written or electronic form and follows the minimum requirements when the accounting firm acts as a processor in accordance with Article 28 of Regulation (EU) 2016/679.

The third stage is the performance of the contract, which is carried out in accordance with accounting, tax, administrative, and social security legislation. The purposes, means, and measures for data protection are determined by the client or the company in compliance with the applicable provisions.

The fourth stage (termination of the contractual relationship) is governed by contract law and by legislation in the field of the ZMIP and ZMF. The minimum storage periods are set by law, but accounting firms may extend them for the purposes of protection in proceedings under the Criminal Code.

The Personal Data Protection Regulation applies only to natural people. However, by virtue of authorization from the client, accounting firms process

personal data on natural persons obtained from the client, public sources or public authorities.

In sub-point **2.2 Differentiation of activities in specialized accounting firms for the purposes of data protection regulations based on interaction and communication with suppliers and other contractors (lenders and borrowers)**, a more detailed analysis of the establishment and performance of contractual relationships with the category of suppliers and other counterparties is carried out as follows:

- landlords within the meaning of Article 228 of the Obligations and Contracts Act;
- lenders and borrowers pursuant to Article 243 of the Obligations and Contracts Act;
- persons exercising a liberal profession within the meaning of paragraph 1, item 29 of the additional provisions of the Personal Income Tax Act;
- natural persons employed under non-employment legal relationships within the meaning of paragraph 1, item 30 of the Personal Income Tax Act.

The selection of these categories is determined by the usual contractual relationships of specialized accounting firms. When interacting with suppliers and external people, the company acts as a personal data administrator, independently determining the purposes of their processing in accordance with the legislation in the field of personal data protection.

The source of the data is the subject itself – a supplier or other external party with whom the enterprise has a contractual relationship. The types and categories of data, the periods for their storage, and the circle of recipients are defined by law. Recipients of the data may be public authorities and state administration bodies.

Subsection **2.3, Differentiation of activities in specialized accounting firms for the purposes of data protection legislation with staff**, analyzing the specific economic activity of the firms and the function of accounting. For the purposes of staff selection and appointment, as well as for the performance of employment relationships, specialized accounting firms process personal

data based on the Labor Code and applicable regulations. The processing aims to fulfill contractual and legal obligations, as well as to protect legitimate interests (Regulation (EU) 2016/679).

The volume of data collected requires a clear definition of its sources, categories, storage periods, location, protection measures, and recipients. The categories include identification data, information on remuneration, benefits and social benefits, human resources movement, job and contract information, as well as a special category of data. The storage periods are regulated by accounting and social security legislation, and the main recipients are state institutions and judicial authorities in labor disputes.

The staff of the accounting firm acts as data processors under the direction of the controller – the company's manager. In this capacity, the firm is required to include confidentiality clauses in employment contracts, which remain in force even after the termination of the legal relationship.

The Regulation requires controllers to assess the risks associated with the processing of personal data and to implement adequate organizational and technical measures to ensure security and confidentiality. Therefore, the following section examines measures for the protection of personal data that are relevant to the activities of specialized accounting firms.

Subsection **2.4 Measures for protecting information when processing personal data by specialized accounting firms** examines the guidelines proposed by the Regulation for appropriate practices for protecting data confidentiality, as well as good practices proposed by some authors (Weisel 2021; Scharnick 2018). Finally, appropriate measures for the protection of data subjects relevant to the accounting sector are summarized as follows:

- physical measures – restricted and controlled access to buildings, premises, documents, and equipment through locks, cabinets, security, and fire protection systems;
- documentary measures – internal rules, instructions and procedures, registers, training records, risk assessment and their impact on security, as well as monitoring and certification;

- Organizational measures – regular training and certification of personnel, monitoring of compliance with rules, a "clean desk" policy⁸ , and regulated access to documents and devices;

- Cryptographic measures – use of appropriate hardware and licensed software for data encryption.

Documenting these measures is a key means of demonstrating compliance with regulatory requirements and the principle of accountability. In this regard, companies may appoint or hire a data protection officer to assist with the compliance process and ensure that adequate policies and procedures are in place. The role, functions, tasks, personal and professional qualities of the data protection officer must be thoroughly understood in order to be performed with the necessary quality and professionalism. Therefore, the following section analyzes the functions of the person under review in performing their role as a personal data protection officer, considering whether they are part of the company's staff or an external person.

3. Functions and requirements for data protection officers in accounting firms

The data protection officer plays a key role as an advisor on compliance with personal data protection rules and as an intermediary between supervisory authorities, data subjects, and the organizations that appoint them. According to Article 37(1) of Regulation (EU) 2016/679, the appointment of an officer is mandatory only in certain cases. The dissertation research assumes that accounting firms, although they process special categories of data, should not automatically be considered "large-scale processors" and are therefore not required to appoint a data protection officer.

⁸ The "clean desk" policy means that documents are stored in designated places protected from unauthorized access as soon as work on them is completed.

However, controllers or processors may voluntarily appoint such a person for the purpose of achieving a higher level of compliance.

According to Article 37(5) of Regulation (EU) 2016/679, the data protection officer must have the appropriate personal qualities, professional qualifications, and experience, including expert knowledge of data protection, competence in the field of IT security (European Data Protection Supervisor, 2005: 3–4) and a good understanding of the specifics of the organization. Proof of this knowledge is usually based on training and certification programs that meet the requirements of the Regulation and ISO 17065.

At present, there are no accredited organizations or training centers in Bulgaria that provide certified training in this area. At the European level, regulation varies from recommended courses to accredited certification (see Table 1).

Table 1. Overview of data protection certification regulations in selected European countries

<i>Country</i>	<i>Accredited certification body</i>	<i>Obligation to certify DPO</i>	<i>Training/qualification</i>
<i>Poland</i>	No	No	Numerous educational activities; postgraduate qualification agreements with universities
<i>Spain</i>	yes	no	List of educational institutions with recognized training programs
<i>Italy</i>	Yes	no	Accredited certification according to UNI 11697
<i>France</i>	Yes	no	Accredited certification according to an established reference system
<i>Germany</i>	no	no	Various forms of training

Source: author's research

As a result of the above, the presented good practices justify the conclusion that it is appropriate for personal data protection officers in Bulgarian accounting firms to have the opportunity for voluntary certification by an accredited certification body (in accordance with the Personal Data Protection Act and the Personal Data Protection Regulations). In addition, training should be carried out in accordance with approved educational programs and with clear criteria for improving knowledge, skills, and proving professional qualifications for practicing the profession after passing a formal exam.

The procedure for performing the tasks of the data protection officer includes familiarization with the overall organizational structure of the enterprise, creation of data processing registers, participation in the preparation of risk assessments, etc. (see Figure 1)

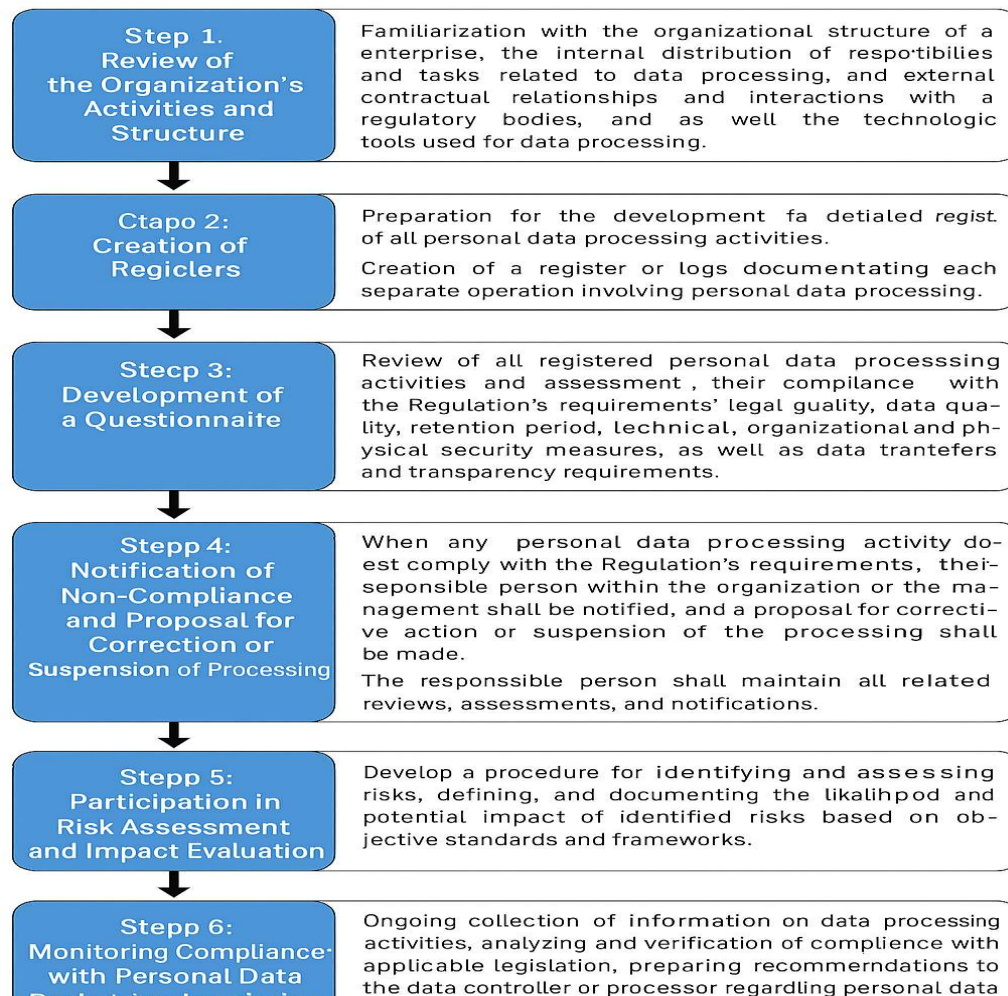


Figure 1. Procedure for performing the tasks of the data protection officer

Source: author, based on Korf and Georges (2019)

The data protection officer may be hired externally, or the position may be combined with another position within the organization. Due to the fact that the person under investigation cannot hold managerial functions that determine the purposes and means of processing, in accounting firms, it is almost impossible to combine the position. Often, departments in accounting firms consist of one person who is also the manager, and in this sense, there

is a potential conflict of interest and an inability to comply with the principle of independence. Therefore, it is more appropriate for accounting firms to avoid combining the position as an option for exercising the role.

One of the main tasks of the data protection officer is to assess the risks associated with the processing of personal information. The provisions of Regulation (EU) 2016/679 require the involvement of this person mainly in the impact assessment, but it is recommended that they also cooperate in the overall risk assessment process by providing expert advice (Article 35 of Regulation (EU) 2016/679).

The assessment includes an analysis of the likelihood of a security breach and its impact on the rights and freedoms of data subjects. The Regulation requires controllers to reduce risks to an acceptable level through appropriate organizational and technical measures, which implies a systematic assessment of each processing operation.

Even in cases where accounting firms are micro-enterprises and do not process large volumes of personal data or special categories of data, conducting a risk assessment remains a key element in complying with the regulatory framework and limiting potential damage.

Risk analysis methodologies can be qualitative or quantitative. There are various frameworks for assessing security risks that can also be applied in accounting firms, the most popular of which are⁹ OCTAVE Allegro, ISO/IEC 27005, and NIST 800-30, which include three key steps: risk analysis, risk assessment, and business impact assessment.

- OCTAVE Allegro (Operationally Critical Threat, Assets and Vulnerability Evaluation) is asset-oriented, emphasizes subjective assessment of consequences, and places less focus on uncertainty measurements;

- ISO/IEC 27005 offers a consistent approach to risk identification, including assets, threats, controls, vulnerabilities, consequences, and

⁹ As WANGEN et al. (2017, p. 685) point out, there are over fifty citations in the academic literature for the above frameworks.

probability. It contains predefined criteria and matrices for assessment and prioritization (Wangen et al. 2017: 692–693);

- NIST 800-30 focuses on threats but does not cover assets and stakeholders; risk is calculated by comparing probability and consequences.

According to the literature and ENISA recommendations (2022a), the most comprehensive approach to personal data protection is ISO/IEC 27005 (ENISA 2022a; Wangen et al. 2017). This framework is suitable for accounting firms as it provides a clear and applicable method that complies with regulatory requirements.

The purpose of a data protection impact assessment is to:

- identify high risks in data processing;
- assess their likelihood and severity;
- introduce adequate measures to mitigate them;
- document the process and demonstrate compliance with the regulation (Korf and Georges 2019: 244).

Alternatively, other established risk management methodologies, such as ISO 31000, may be used.

Adherence to an approved code of conduct or certification mechanism may serve as evidence of compliance with the Regulation. For this reason, the data protection officer may recommend joining such initiatives. Although the Code of Conduct is essentially a voluntary document aimed at facilitating the effective application of the Regulation in certain sectors or professions, as of February 2025, there are no documents approved in Bulgaria in accordance with the requirements of the Regulation. The reason for this is the lack of the necessary regulatory conditions, namely the absence of an accredited data protection supervisory authority (Article 41(1) of Regulation (EU) 2016/679).

In summary and conclusion, the implementation of control in accordance with personal data protection legislation should be viewed not as a one-off act, but as a continuous process that could be most effectively carried out by data protection officers. They must carry out preliminary/preventive control within the organization in a professional and

competent manner and in partnership with the supervisory authority. To this end, the data protection officer in specialized accounting firms should have the necessary knowledge, experience and personal qualities. These are developed based on adequate training provided by an organization, university or other institution accredited for these purposes. In this regard, it is appropriate to examine and analyze how accounting firms currently fulfill their obligations in the field of personal data protection and information security. This allows for a more in-depth understanding of the need to introduce a qualified data protection officer, as well as to develop a model and procedures for compliance with the requirements of the legislation, tailored to the specific needs of accounting firms.

The following research tasks, presented in the introductory part of the study, are addressed in the second chapter:

- a distinction is made between accounting activities in specialized companies based on the transactions and events carried out with people internal and external to the reporting entity. Of all external persons, a more in-depth analysis is carried out on relations with customers, suppliers, and certain other external persons. From the group of internal people, the analysis focuses on the staff of the enterprises;

- appropriate practices are examined concerning personal information security measures relevant to the accounting sector.

CHAPTER THREE. Study of the measures and procedures applied in accordance with the regulatory framework for personal data protection by specialized accounting firms in Bulgaria

The third chapter provides a systematic analysis of the practices applied in the accounting sector, identifies effective approaches to personal data protection, and assesses the impact of digitization on information security and

confidentiality. This includes a study of the application of good practices by accountants to ensure security in accordance with regulatory requirements.

In pursuit of the thesis's objective, the chapter presents three empirical studies conducted among practicing accountants from specialized accounting firms. The main objective of the studies is to collect and analyze empirical data to complement the theoretical analysis and support the verification of the author's hypotheses. They focus on the impact of digitization and the use of innovative software solutions in accounting, as well as on the risks to personal data security and the necessary technical and organizational measures for their protection. To achieve this goal, a combined approach was applied, including two questionnaire surveys and semi-structured in-depth interviews. The first questionnaire survey focuses on the measures and procedures currently applied by specialized accounting firms to protect personal information. The purpose of the second survey is to analyze trends in digitization and innovation in accounting firms and to assess the associated risks to personal data, expanding the analysis with additional quantitative data. The third study, conducted through semi-structured in-depth interviews with accountants, aims to validate and verify the results of the previous two studies and provides a qualitative explanation of the quantitative results. This approach allows for a deeper understanding of specific cases, problem areas, and good practices related to the implementation of digital tools and the application of personal data protection requirements in accounting firms.

In section **1. Research Methodology and Author's Hypotheses**, the methodological framework of the empirical studies conducted is presented, aimed at analyzing the impact of digitization and the use of innovative software solutions on accounting activities and the processes of collecting, processing, and storage of personal data in specialized accounting firms. It includes the characteristics of the methods used for data collection and analysis, the criteria for selecting respondents, as well as the author's hypotheses formulated based on the theoretical analysis in the previous sections.

First, the author conducted an anonymous online survey of the measures and procedures currently applied by specialized accounting firms to protect personal information, carried out between February 9, 2021, and May 8, 2022. The survey form was distributed online via Google Forms and consisted of 44 open and closed questions, grouped into four groups. The survey involved 107 respondents, selected at random using the response method. The target group consists of accounting firms and their employees, members of a professional accounting organization – the Institute of Professional Accountants in Bulgaria.

Many authors point out that no clear and specific guidelines are provided for compliance with regulatory requirements (Hoofnagle et al. 2019), including a complete description of appropriate technical, organizational, and documentary measures to protect information. The Regulation recommends "regular testing, evaluation, and assessment of the effectiveness of technical and organizational measures to ensure the security of processing" (Article 32, paragraph 1, point (d) of Regulation (EU) 2016/679). Therefore, identifying the risks of processing individual information (including cyber risks) and assessing them is an important factor in choosing specific measures and practices for the protection of personal data. These practices include encryption and monitoring, testing, and evaluating the effectiveness of technical and organizational security measures. To analyze these factors, the following hypotheses are formulated for testing within the study:

(H1) There is a statistically significant relationship between the accounting sector's susceptibility to cyberattacks leading to personal data leaks and the use of email encryption;

(H2) There is a statistically significant relationship between the vulnerability of accounting firms to cyber-attacks leading to personal data leaks and the existence of monitoring, testing, and evaluation of the effectiveness of technical and organizational security measures.

To test the hypotheses, X^2 analysis of statistical relationships and dependencies by Cramer was used.

The limitations of the first study, related to the lack of focus on accountants' perceptions of cyber risks and threats to personal data security, necessitate a second study. It aims to expand the analysis by examining the relationship between digital transformation in accounting firms and perceived information security risks. A new questionnaire with 14 questions was developed. The Google Forms application was used to collect responses. The survey was conducted between October 11, 2023, and November 19, 2023. The target group consisted of accountants representing accounting firms and their employees.

The hypothesis in the study is based on literary sources that examine the relationship between technology, risk management, and information security in accounting. Ensuring the integrity of data subjects' information is becoming a priority, as digitization and globalization create conditions for risks of harm to individuals (Gonçalves et al. 2022; Lehenchuk et al. 2022; Datenschutzkonferenz (DSK) 2018). In view of the above, the increase in cyber risk, respectively the threat to the integrity of personal data from the use of digital tools for collecting, processing, and storing information in accounting, is a factor that needs to be investigated. To analyze this factor, the following hypothesis is formulated:

(H3) There is a statistically significant relationship between the implementation of digital solutions based on new digital technologies for the collection, processing, and storage of data by specialized accounting firms over the past two years and an increase in cyber risks to the confidentiality of information in the sector under review.

To test the hypotheses, X^2 analysis of statistical relationships and dependencies by Cramer was used.

The study focuses on the current state of digitization, automation, and innovation in accounting firms in Bulgaria and the risk to the confidentiality of personal data from the use of new technologies. The study does not consider factors that may influence the digitization of accounting firms, such as the geographical location of the business, gender, age, length of service in the profession, and motivation to improve the ICT knowledge and skills of accountants.

Appropriate scientific methods need to be applied to validate the results of the two surveys and gather more in-depth information on the opportunities for improving and maintaining the professional competence of accountants in the field of personal data protection. These include conducting in-depth interviews with representatives of the sector under study. The interviews follow a script that combines pre-defined questions related to the key topics of the study with the possibility of free responses and expanding the discussion on specific cases. This ensures a balance between the focus of the research and the flexibility to explore new aspects raised by the respondents.

The semi-structured in-depth interviews were conducted with 10 participants between June 7, 2024, and June 16, 2024. The interviewees were selected on the basis of their professional qualifications, professional experience in the field of accounting, and knowledge of personal data protection in specialized accounting firms. The target group consists of practicing accountants who represent and manage accounting firms or are employed by them. The aim is to analyze in depth the specific challenges associated with the implementation of digital technologies and compliance with personal data protection regulations.

The semi-structured interviews play a validating and enriching role within the methodological strategy of the dissertation, providing a deeper understanding and confirming the empirical validity of the formulated hypotheses.

In point **2. Results from empirical studies**, the results of the conducted surveys and semi-structured in-depth interviews are presented and analyzed.

The main objective is to summarize the identified trends, validate the formulated hypotheses, and supplement the quantitative data with qualitative observations from the practice of accounting firms.

Subsection 2.1 *analyzes the relationship between assessing and identifying the risks of processing individual information (including cyber risks) and the choice of specific measures and practices for protecting personal data.*

Based on the collected and analyzed data and using the selected methodology for testing statistical relationships and dependencies, it is indicated that there is a weak statistically significant relationship between the investigated potential risk to information security and encryption in relation to electronic communication (see Table 2). Taking into account the existence of a higher level of risk to data security during processing (such as unauthorized disclosure or access to personal data that has been transferred, stored or otherwise processed), the companies surveyed take appropriate measures in accordance with the legislative proposals. The aim is to reduce, limit or exclude the possibility of unwanted threats occurring.

Table 2. Hypothesis testing (H1) – Statistical relationships between the use of email encryption and respondents' views on the accounting sector's vulnerability to cyberattacks

Variable	f	Level of Significance (α)	Chi-Square Value	Cramé r's V	P-Value
Encryption of email communication		0.05	7.47	0.26	0.006

n=107

A statistically significant correlation is confirmed between respondents' perception of the accounting sector's vulnerability to cyber-attacks and the

existence of testing and evaluation of the effectiveness of the measures put in place in enterprises, although the correlation found is weak (see Table 3).

Table 3. Hypothesis testing (H2) – Statistical correlations between the existence of monitoring, testing, and evaluation of the effectiveness of technical and organizational security measures and respondents' perception of the accounting sector's vulnerability to cyberattacks

Variable	f	Level of Significance (α)	Chi-Square Value	Cramer's V	P-Value
Monitoring, testing, and evaluation of the effectiveness of technical and organizational security measures		0.05	3.90	0.19	0.04

n=107

In summary, the hypotheses derived from the analysis of the specialized literature in Chapters One and Two are confirmed by the results of the empirical study of specialized accounting firms in Bulgaria.

Subsection 2.2 analyzes the relationship between the implementation of innovative digital tools for collecting, processing, and storing data by specialized accounting firms and the increase in cyber risks to confidentiality of information.

The analysis of the data collected from the second survey, based on the methodology applied for assessing statistical dependencies, does not establish a statistically significant relationship between the implementation of innovative digital tools for data processing by specialized accounting firms over the last two years and the increase in cyber risks affecting the confidentiality of information. (see Table 4)

Table 4. Hypothesis testing (H3) – Statistical dependencies between the implementation of innovative digital tools for data collection, processing, and storage over the last two years by specialized accounting firms and the increase in cyber risks to information confidentiality

Variable	df	Level of Significance (α)	Chi-Square Value
Implementation of innovative digital tools for data collection, processing, and storage over the last two years.	1	0.05	1.24

n=212

In summary, the hypothesis put forward in the analysis of the specialized literature in Chapter One of the dissertation is not confirmed by the results of the empirical study conducted among specialized accounting firms in Bulgaria.

The results of the second study do not answer the question of what the basis for the respondents' opinion that new technologies (cloud accounting solutions and others) in accounting is significantly increase cyber risk and information confidentiality. The reason for the low level of digital literacy is also beyond the scope of the study, given that unfamiliarity with specific technological solutions and tools hinders their application in the sector under review. The latter is a possible factor for the weak application of pseudonymization and encryption as appropriate means of protecting personal information. In view of the above, there is a need for a more in-depth study focused on analyzing the identified factors.

In order to validate the results of the two surveys and collect more in-depth information on the possibilities for improving and maintaining the professional competence of accountants in the field of personal data protection, it is necessary to apply appropriate scientific methods. These

include conducting in-depth interviews with representatives of the sector under study.

Subsection **2.3** *examines the opportunities for improving and maintaining a high level of competence and professional skills in personal data protection on the part of accountants.*

The results of the semi-structured in-depth interviews once again validate the hypotheses set out in the dissertation research that assessing the risks of personal data processing when using innovations in accounting is a prerequisite for choosing appropriate technical, organizational, documentary, and personal measures for the protection of personal data. The participants in the study confirm the assumption that the interpretation of specific regulatory postulates by accountants is an obstacle to the reliable and effective application of information protection rules. The establishment of certification training by accredited organizations for data protection officers helps them perform their tasks and demonstrate professional experience and knowledge, according to our study. The development of and adherence to a Code of Conduct in the accounting sector is viewed positively as a means of overcoming problems and obstacles in compliance with the regulations by specialized enterprises. The results of the semi-structured in-depth interviews provide useful information regarding the information channels through which accountants learn about developments in the sector, specific difficulties in understanding legislation in the field of confidentiality, and the reasons for the claim that there are cyber risks associated with the use of digital tools for processing and storing personal data.

The study does not analyze issues related to preventive and subsequent control by supervisory authorities and their impact on the motivation of staff in specialized accounting firms to deepen their knowledge and skills in the field of information protection legislation.

Subsection **2.4** *presents summaries of the three empirical studies and a discussion.*

The analysis of the results of the questionnaire surveys and semi-structured interviews reveals a number of weaknesses in the practices of specialized accounting firms with regard to personal data protection. Violations of the principles of storage limitation and accountability, lack of risk assessments and regular training, absence of systematic testing of measures, and limited use of encryption and pseudonymization have been identified. The reasons for these shortcomings are related to the complexity of the regulatory framework, insufficient digital skills, lack of confidence in the effectiveness of the measures, and limited resources for training.

On this basis, the following recommendations are formulated, arranged according to the specific studies:

From the first survey:

- preparation of records of processing activities with clearly defined retention periods;
- conduct individual risk assessments using the ISO/IEC 27005 matrix;
- regular staff training on policies, measures, and risks;
- systematically test and evaluate the effectiveness of security measures (Article 32(1)(d) of Regulation (EU) 2016/679);
- introduction of policies for encryption of communications and restriction of access to data, including secure deletion.

From the second survey:

- improving digital competences and ICT skills through training courses organized jointly with accounting software providers;
- promoting national digitization programs and funding opportunities for digital solutions;
- developing knowledge of cybersecurity and practical application of good risk management practices.

From the semi-structured in-depth interviews:

- wider dissemination of information on training in ICT, cybersecurity, and data protection through professional organizations and social media;

- holding regular voluntary training courses organized by accredited institutions with clearly defined certification criteria;
- development of a Code of Conduct for the accounting sector by an industry organization, tailored to the specific nature of the activity and regulatory requirements.

In conclusion, although current practices do not guarantee full compliance with the legislative framework, there is a clear willingness in the sector to improve through process systematization, digital transformation, and upskilling.

The summarized results highlight the need for a systematic approach, which requires the development of a Code of Conduct tailored to the specific challenges and needs of accounting firms. In view of the above, the following section offers recommendations for the development of a code that corresponds to the findings and analyses of the dissertation research.

In point **3. *Recommendations for the development of a Code of Conduct for the accounting sector in the context of personal data protection***, the approval criteria set out in Article 40 of the Regulation are taken into account. The adoption of a Code of Conduct by accountants represents a proactive approach to harmonizing personal data protection standards, providing clear guidelines for good practice in the sector. The code may be developed by an industry organization such as the IPSB. Provided that a code is developed in accordance with the established criteria, it is possible to obtain approval from a supervisory authority, which guarantees its applicability and compliance with regulatory requirements.

Based on the conclusions drawn from the analysis of the specialized literature, the surveys, and the semi-structured in-depth interviews, ***recommendations are made for the development of a Code of Conduct for the accounting sector by a professional organization regarding:***

- general criteria and mechanisms for performing risk analysis and impact assessment under Article 35 of the Regulation;

- a description of the categories of personal data and/or registers containing personal data, the methods of collection, processing, and storage of personal data, including the legal basis and a description of the legitimate interests of the controller and processor of personal data, where applicable;
- a description of the safeguards for fair and transparent processing of personal data;
- the technical and organizational measures for protection and the conditions for applying pseudonymization of data, if applicable.

Chapter Three fulfills the research task set out in the introduction to the dissertation, namely, to make recommendations for the development of a Code of Conduct that considers the specific features of personal data processing in accounting.

Conclusion

Digitization and new digital technologies are making their presence felt in all areas of the modern economy. In "some sectors, the introduction of innovations is faster and easier than in others" (Dimitrova 2021: 42). The accounting sector carries out its activities using various software technologies, but there are still barriers to the wider use of innovation and the automation of operational and routine processes. On the other hand, the introduction of innovations creates risks for the sufficient protection of personal data. Identifying potential threats is a prerequisite for selecting and applying appropriate means to prevent unauthorized and unlawful access to personal information and the violation of individuals' rights. To this end, the correct interpretation of regulatory requirements and the establishment of effective procedures, security and monitoring measures, as well as the correct identification of individual information flows, are the basis for compliance with the legislative framework and the prevention of possible damage¹⁰. In

¹⁰ for data subjects, for accounting firms themselves, for business in general

this context, the role of the data protection officer is leading in the implementation of preventive, regular, and administrative control and consultation. Their professional competence and personal qualities must be proven in order to ensure confidence in their ability to perform their functions and tasks for the benefit of the organizations that have entrusted them with this responsibility. On the other hand, the creation and approval by a competent authority of a Code of Conduct for the accounting industry contributes to a greater extent to the harmonization of the regulatory postulates by accountants.

All of the factors listed above that support the Bulgarian accounting sector in the implementation of personal data protection legislation are examined and analyzed in detail in this dissertation.

The conclusions drawn **in Chapter One** confirm *the hypotheses* set out in the dissertation research that:

- digitization and the use of new technological software solutions in accounting create risks to the security and confidentiality of personal data handled by accountants;

- identification and assessment of the risks of personal data processing when using new digital solutions in accounting requires the use of appropriate and adequate proactive measures to protect the information of data subjects (e.g., encryption and others);

- interpreting the complex regulatory regime for the protection of personal data by accountants in accounting firms is difficult due to the lack of clear, specific, and comprehensive guidelines;

- The role of accounting firms in Bulgaria, as data protection officers, in preventing damage to organizations and individual clients is essential for limiting financial and other abuses and imposing administrative sanctions.

One of *the main contributions* of **Chapter One** is the in-depth literature review of the definitions used in the field through the prism of accounting, and the proposal of a definition for the terms "data" and "information." The proposed definitions of the concepts are useful for the correct understanding,

interpretation, and application of the complex regulatory regime in the field of confidentiality by accountants in connection with the performance of their duties.

The second chapter presents a study of the specific features of the application of the personal data protection regime in accounting. Based on the information collected and analyzed in the chapter, **the following main conclusions** are drawn:

- the identification and assessment of the risks of personal data processing is a prerequisite for the selection of appropriate technical, organizational, documentary, and personnel measures at the system design stage and, by default, for compliance with the regulatory framework for the protection of data subjects' information (e.g., encryption and others);
- the introduction of certification training by accredited organizations to ensure that data protection officers acquire up-to-date and sufficient knowledge guarantees a higher degree of compliance with the tasks of maintaining an adequate level of protection and security by organizations;
- Developing and adhering to a Code of Conduct for the accounting sector contributes to the fulfillment of obligations under personal data protection legislation, reflecting the specifics of the industry.

The second chapter of the study formulates a recommendation for the adoption of a risk assessment framework matrix for the processing of personal data that is appropriate for the accounting sector, which assists accounting firms in the method of fulfilling their obligations. In addition, at this stage, practices approved for application for training data protection officers in some European countries are being studied. On this basis, it is recommended that data protection officers in Bulgarian accounting firms have the option of voluntary certification by an accredited certification body, as provided for in the Personal Data Protection Act and the Personal Data Protection Regulations. Training should be carried out in accordance with approved educational programs and with clear criteria for improving knowledge, skills, and proving professional qualifications for practicing the profession after

passing a formal exam. *A major contribution* is the proposed model for describing the registers of personal information processing based on transactions and events with people internal and external to the reporting entity.

Chapter **Three** presents an empirical study of the measures and procedures applied in accordance with the regulatory framework for personal data protection by specialized accounting firms in Bulgaria. Based on the results of questionnaire surveys and semi-structured interviews, **scientific research contributions** with practical applicability for accounting firms are presented.

First, a direct correlation is identified between the performance of a formalized risk assessment and the implementation of specific protective measures. This provides grounds for the application of internal risk assessment methodologies as a condition for selecting appropriate technical and organizational solutions – a practice that can be implemented by both small accounting firms and larger companies.

Second, there is a justified need to introduce voluntary certification training for data protection officers. This training should be conducted by accredited organizations, according to pre-approved programs, and should conclude with a formal exam. This proposal opens up the possibility for standardized professional training that complies with data protection legislation requirements and can be applied as a good example within the professional community.

Third, practical guidelines have been formulated for the development of a Code of Conduct for the accounting sector, which can be developed and implemented by industry organizations. The code includes mechanisms for identifying risks, categorizing data, selecting appropriate protection measures, and ensuring transparency in the processing of personal information—tools that can become an established professional standard in the sector.

In summary and conclusion, digitization in accounting leads to an increase in the risks associated with the processing of personal data of individuals. Specialized accounting firms often lack sufficient resources and internal mechanisms to adequately assess and manage these risks. Accountants' limited awareness of regulatory requirements and the capabilities of modern technologies contribute to non-compliance with the legal framework and increases the likelihood of security breaches and confidentiality violations. The dissertation identifies key dependencies between risk assessment and the implementation of appropriate protective measures, offering practical guidelines to assist accounting firms in making informed decisions. Furthermore, it argues about the need for certified training for data protection officers conducted by accredited organizations to improve professional competence and ensure the sustainable application of the principle of accountability in the sector.

The hypotheses confirmed in the dissertation research support the thesis that digitization in accounting poses risks to personal data that require systematic legal analysis and application of the principle of accountability to develop effective information protection practices.

In future studies, it would be appropriate to analyze the knowledge of representatives and employees in accounting firms regarding the capabilities of existing technological solutions for data analysis and processing. This is particularly important as delays in digitization and automation processes may result from a lack of awareness or misunderstanding of their functionalities.

The dissertation can serve as a basis for the improvement and development of further research and future developments on the topic related to the possibility of introducing innovations in the accounting sector and their impact on the protection of personal information in the context of applicable legislation.

IV. List of publications related to the topic of the dissertation

1. Studies

•MITKOVA, M. 2021. Practical-Applied Analysis of the Processing of Personal Data in the Accounting Activities. Research Papers of IBS, vol. 13, IBS-Press, pp. 122–158. ISSN 1313-0846

2. Articles

•MITKOVA, M.; GEORGIEVA, D. 2022. A Study of Accounting Activities in the Context of Personal Data Protection. Research Papers of IBS, vol. 14, IBS-Press, pp. 93–107. ISSN 1313-0846

•MITKOVA, M. 2023Implementation of Digital Tools and Innovations in Accounting Practice – Opportunities and Prospects. ICPA, No. 3. [online]. Available at: <https://www.ides.bg/e-journal/2023/issue-3/03-2023-milena-MITKOVA>.

3. Reports

•MITKOVA, Milena. 2025. European integration and the need to use innovative technologies in accounting, Economic Development and Policies: Realities and Prospects. European Integration, Convergence and Cohesion. Sofia: ERI at BAS, p. 426-430, ISBN 978-954-9313-27-7

V. Summary of the main contributions in the dissertation

The main contributions of the dissertation can be summarized as follows:

•an in-depth theoretical analysis of the concepts of "information," "data," and "personal data" is carried out, and a definition of "data" and "information" for accounting purposes is provided in the context of the regulatory framework for the protection of personal information;

- from a theoretical and applied perspective, a model is proposed for describing the registers of personal data processing for the accounting sector, based on the transactions and events carried out with people internal and external to the reporting entity;

- A direct relationship has been identified between the performance of a formalized risk assessment and the implementation of specific protective measures. This provides grounds for the application of internal risk assessment methodologies as a condition for selecting appropriate technical and organizational solutions—a practice that can be implemented by both small accounting firms and larger companies;

- The need to introduce voluntary certification training for data protection officers is justified. This training should be conducted by accredited organizations, according to pre-approved programs, and should conclude with a formal exam. This proposal opens the possibility for standardized professional training in line with data protection legislation requirements and can be applied as a good example within the professional community;

- Practical guidelines have been formulated for the development of a Code of Conduct for the accounting sector, which can be developed and implemented by industry organizations. The code includes mechanisms for identifying risks, categorizing data, selecting appropriate protection measures, and ensuring transparency in the processing of personal information—tools that can become an established professional standard in the sector.

VI. Declaration of originality

I declare that this dissertation research is entirely my own work and that no foreign publications or developments have been used in violation of their copyright.