sciendo

FINANCIAL SCIENCES. NAUKI O FINANSACH
Year 2019, Vol. 24, No. 3
ISSN 2080-5993
e-ISSN 2449-9811

PROTECTION OF PERSONAL DATA IN THE SYSTEM OF MODERN ACCOUNTING IN THE CONTEXT OF THE IMPLEMENTATION OF THE REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE EU COUNCIL 2016/679 OF 27 APRIL 2016

Katarzyna Świetla
Cracow University of Economics, Cracow, Poland
e-mail: kswietla@uek.krakow.pl

ORCID: 0000-0001-7796-93-79

DOI: 10.15611/fins.2019.3.06
JEL Classification: M41, I25.

Summary: This article is an attempt to analyze the existing solutions in the field of the protection of personal data. Training and advisory materials on this subject prepared by numerous law firms (32) were analyzed, providing a valid explanation, understanding and implementation of the new obligations in the field of data protection. In addition the author conducted pilot interviews in accounting offices (17) concerning the protection of personal data to indicate the approach of service providers to the performance of the tasks in the field of personal data protection. The key findings of the study are: noticeable increase in the interest of the contracting parties in data protection issues, as well as presenting their positive aspects along with possible problems in their practical application. An important contribution of the author is also the presentation of the key points of agreements which the parties should pay attention to in order to avoid misunderstandings.

Keywords: accounting, accounting services, data protection, behavior of service providers.

1. Introduction

The modern approach to accounting commonly indicates its practical function, which is to provide users with information to make correct decisions and to hold managers accountable for managing the assets of their organizations, and hence the generated results. As has repeatedly been noted, accounting on a global scale is treated as the language of business, leading to its convergence for transnational audience expectations. The internationalization and globalization of business and the related flows of information result in the need for the protection of personal data being processed and transferred in order to secure the interests of users. As noted by

N. Artieniewicz [Artieniewicz 2018], the general view of accounting depicts it as dealing with facts, regulations, and dry numbers alone and where their treatment is not considered as human behavior, which should be reasonable, but it is not always so. Financial and accounting processes should also be seen as including human beings, their qualities, motives, consistency of behavior, decisions, attitudes and individual circumstances. According to the author of this article, they will have a definite influence on the correct understanding and application of EU Regulation 2016/679, which was implemented by individual countries in the form of the provisions in their regulations.

This article is an attempt to analyze the existing solutions in the field of personal data protection regarding the above-mentioned Regulation, the Act of May 10, 2018 and the provisions adopted by entities and institutions subject to them, providing services in the field of accounting (accounting offices), tax advisory and audit. It should also be emphasized that the correct implementation of the provisions depends on the actions of the people using them and their diligence in this respect, which undoubtedly has its roots in the perception of accounting through its behavioral prism.

The methods adopted for the research were: critical analysis of the available literature and source documents prepared for the implementation of GDPR solutions, and direct interviews.

Training and advisory materials on this subject prepared by numerous law firms (32) were analyzed, providing a valid explanation, understanding and implementation of the new obligations in the field of data protection.

In addition the author conducted pilot interviews in accounting offices (17) concerning the protection of personal data, to indicate the approach of service providers to the performance of the tasks in the field of personal data protection. However, due to the fact that the new regulations had not been introduced until recently, they did not bring significant results extending beyond the recommendations proposed by the accounting firms. The hypothesis put forward for the purposes of this study was whether there would be an increase in the awareness of the contracting parties with the expiry of the validity of the GDPR solutions. At the time of commencement of the study, representatives of the offices declared unanimously that they were only at the stage of investigating the regulations and that reflection will come at a later stage.

2. GDPR regulations

On 28 May 2018, in Poland and other European Union countries, a regulation on the protection of personal data commonly referred to as the GDPR came into force. Regulation (EU) 2016/679[1] of the European Parliament and of the Council

[1] Hereinafter referred to as the Regulation.

of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation). It should be emphasized that the Regulation on the protection of personal data is a new EU legal act which aims to strengthen and harmonize data protection laws across the European Union. In addition, it aims to provide solutions to improve the Member States' preparation for the rapid changes caused by developing technologies, especially in the field of data transmission and processing by those responsible.

GDPR, however, leaves many issues to the internal regulations of the Member States. This includes the organization of regulatory bodies, certification, the conduct of proceedings before the supervisory authority, the amount of financial penalties and the additional sanctions in case of non-compliance with data protection law. Against this background, the Polish authorities have developed an appropriate law on the protection of personal data, namely the Act of 10 May 2018 on Personal Data Protection [The Act of 10 May 2018…] announced on May 24, 2018. The relevant law should be applied to the specific issues forwarded by the EU legislator to be regulated at the level of national laws. The introduced provisions apply directly, which means that they are binding for each economic operator and apply to all individuals without exception on the provision of their services or other business transactions for individuals throughout the European Union, regardless of whether the seat of the economic entity is located in the EU or not. The starting point is, which is not without significance, the offering of services to persons residing in the Union.

The new solution applies to all sectors of the economy, including accounting offices, tax advisors and auditors (often providing accounting services to businesses in addition to services related to taxes and auditing the financial statements), required to protect customer data.

With the right action, when implementing the provisions of the above mentioned Act, on the one hand, an accounting office gains the trust of customers, and on the other, reduces the risk of data leakage and possible financial penalty or even a ban on doing the business in the event of a negative opinion of the Office for the Protection of Personal Data (UODO). This is obviously conditioned by the normal activities and ethics of employees.

According to point 26 of the Regulation, personal information is defined as data concerning an identified or identifiable natural person. To determine whether a person is identifiable, one should take into account any reasonably probable ways (including the identification of entries for the person), for which there is a reasonable probability that it will be used by a controller or other person for the direct or intermediate identification of the individual.

In order to properly protect the personal data, a controller is appointed who is obliged, on the basis of its their knowledge and experience, to assess the risks and evaluate which solutions will be the most correct in the context of the specific nature

of the business entity. The controller also has the obligation to use such technical and organizational measures, which will support the protection of personal data processing. This includes loss, unauthorized access and/or damage.

An example of the actions of a controller can be the obligation to keep a register of processing operations that is not occasional or involves the so-called sensitive data (this does not apply to an entity employing fewer than 250 persons, unless the processing of data can cause a risk of violation of the rights or freedoms of the persons). GDPR rules dictate the need to protect personal data by any of the controllers on the level of data collection and processing system design (i.e. Privacy by design) and at the level of the default settings in the data processing systems (i.e. Privacy by default). The purpose of this requirement is to maximize the protection of personal data at every stage of their processing and within the duration of the responsible controller's role in this task, therefore the controller prepares a draft of the personal data processing system. They should analyze what data will be processed, to what extent, in what period of time and for what purpose.

The assessment of the data also leaves the decision as to the obligation to assess the consequences of his/her actions for data protection (privacy impact assessment) as well as a consultation with the supervisory authority or the appointment of a Data Protection Officer (DPO) to support the controller. They shall be appointed by the controller of the data and the actor providing the data to be processed. The DPO's role has been strengthened thanks to the powers that used to belong to the information security controller (ABI). It should be stressed that the appointment of an inspector has now become the responsibility instead of the earlier privilege of the controller, especially when the main activity of the controller or the processor relates to such processing operations that, because of their sensitivity, scope, purpose and nature and specificity require current, systematic monitoring.

It can therefore be assumed that the important personal data will include:

– name and surname,
– PESEL (citizen identification number) or NIP (tax identification number),
– ID, Internet name,
– address information,
– email,
– other factors: physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

On this basis it must be noted that any operator, including accounting offices, which inherently collect and process data about their customers will be required to implement the requirements of GDPR. This will apply to the stage at which the system is designed (e.g. financial and accounting systems, human resources, tax returns, etc.) where the need to protect customers' personal data has been introduced.

As already emphasized, the responsibility for data protection rests with the controller and the entity processing them. The key action is, therefore, the proper handling of systems using data with privacy as default assumptions.

No matter what requirements are adopted, the method of processing and storing data, and of their proper protection, does not exclude storing them on electronic media, in paper form, or in the cloud or on servers owned by the entity.

Customer trust in the protection of their data is crucial, due to the fact that they entrust their sales and purchase invoices, employee documents, contracts, bank statements, and many other documents relating to the transactions, to the accountancy firm, tax consultant or auditor. This means in effect that they entrust the following to these service providers:

- Information about their contractors (suppliers and recipients).
- Information about the values of their transactions.

In the case of HR services, also:

- Data of employees (including sensitive data, e.g. sick leaves, information on the degree of disability, genetic code, addictions, sexual orientation, ethnic or racial origin, family, religion, philosophical or political views, political affiliation or relationship, court judgments, penalties, fines, etc.).

Regardless of the fact that the documentation has been transferred to the accounting service provider, it remains the property of the operator who purchases the services. Therefore the accounting firm is considered to be the controller of such personal data and it is their obligation to ensure their confidentiality. This obligation is not limited in any way by concluding an agreement on the financial and accounting services. It should be stressed at the same time that the service provider (accountant) for their part is the controller of their employees' data.

In accordance with the provisions of the Regulation, the controller (within the meaning of the controller of personal data) is a natural or legal person, public authority, or entity, which independently or jointly with others determines the purposes and methods of personal data processing. Where the purposes and means of such processing are specified in EU law or in the law of a Member State, a controller may also either be designated within EU law or in the law of the Member State, or specific criteria for their designation may be specified [Regulation (EU) 2016/679…, art. 4 item 7].

On this basis, it should be emphasized that the data controller is obliged, on the basis of their own experience, to assess the potential risks and to estimate which solutions will be optimal to be applied in its business. At the same time, it is incumbent upon the controller to apply technical and organizational measures ensuring the protection of the personal data processed, appropriate to the risks and categories of data covered by the protection. This applies especially to protecting data against unauthorized access, loss, damage or destruction [Szpytko-Waszczyszyn 2017].

Accordingly, the accounting office, tax consultant or auditor has tasks determined by the rules of data protection laws. According to the latest solutions, it is in the interest of the client as a data controller to sign a contract with the accounting office concerning data entrustment. Such an agreement will ensure that the data provided (for which the controller − the client of the office – is still responsible) will

be processed by the entity providing bookkeeping services with due diligence and in accordance with the provisions on personal data protection. In this way it also reserves the use of the data by the entity to which they are entrusted for purposes other than those of the accounting office to which they were provided.

3. GDPR in the practice of accounting offices, tax advisors and auditors

Professionals dealing with accounting perform many tasks, including financial accounting, management accounting, audit, taxes, finance, analysis, control, information processing processes, consulting, and financial management. The implementation of these tasks involves making decisions which, apart from the integration of the data available to them, are also influenced by the emotions, motivations and preferences of such a person, which affects the behavioral aspect of accounting. This includes the role of the persons involved in the processing of data from accounting operations and their relationship to the activities undertaken [Jaworska 2014].

As noted by Birnberg and Shields, the main directions in the area of behavioral accounting are:

- management control,
- collection and processing of data in financial accounting,
- design of information systems in accounting,
- external and internal audit,
- organizational sociology [Birnberg, Shields 1989].

Undoubtedly all these issues fall within the area of the activities of persons employed in accounting offices, tax consultancy and audit, and are a derivative of their decisions and behavior.

Due to the collection and processing of large amounts of personal and financial data, accountancy offices are subject to the obligations arising from the provisions of the GDPR, regardless of the fact that the data controllers are the offices' customers.

For its part, the accounting office is, as has already been emphasized, the controller of its employees' data and also an entity processing the data of its customers in the course of servicing the processes entrusted to it. In such a situation the processing of personal data must, as a rule, take place on the basis of a written agreement. The agreement is based on the provisions of the Regulation, pointing out the need for close cooperation between the controller of personal data and the entity processing them [Trzpioła 2018].

The basis of the service provider's obligation is to secure the data received in formal and technical terms. On this basis, it should be emphasized that when taking over and collecting data sets, the office is obliged to conclude an agreement with the customer confirming the status of data processing rights. Such an agreement will

ensure that the data provided, for which the controller − the client of the accounting firm − is still responsible, will be processed by the entity providing bookkeeping services with due diligence and in accordance with the provisions on personal data protection. Thus, the client of the office (data controller) should use only the services of such processors, which provide sufficient guarantees for the implementation of the technical and organizational measures required by the GDPR.

Ensuring the reliability of accounting offices as to the principles of implementing the requirements of the GDPR can be achieved thanks to numerous recent training courses for employees in this area, which are conducive to its proper implementation. In particular, law firms which examine the scope of activities of their clients and prepare guidelines for the proper application of the GDPR requirements, specialize in the implementation of training and consultancy. They also develop specific agreements on data entrustment, which should define, among other things, the scope of data processing activities. The following are considered to be important:

- name and surname of the employee serving a specific customer or name and contact details of the processor(s),
- the data of each controller (customer of the office) on whose behalf the accountancy office processing their data acts and, where applicable, the representative of the controller or processor,
- the Data Protection Officer's information,
- the classification of the categories of processing carried out on behalf of each controller,
- information about the transfer of personal data to a third country or an international organization if such will be the case (including the name of that third country or international organization),
- a description of the technical and organizational security measures applied in the course of data processing.

As can be seen from the above, the proper implementation of the law requires detailed analysis of the data processing procedures and their basis, rules and security measures applied by those responsible.

As regards the first issue, i.e. the data processing itself, it is important to determine in which processes personal data are involved, whether they have been collected by the processors' own effort or entrusted to them by the client, what the data are and whether there are sensitive data among them. It is also important to recognize the basis for processing the data, the purposes they serve and the processes they concern, as well as the time of their processing. The data processing itself is subject to analysis from the point of view of, among others, their transfer to other entities (e.g. ZUS, US, GUS, etc.), the client's consent, and their awareness in this respect. Moreover, in some situations where, for example, data are entrusted to another entity for the purpose of processing, such a fact should be indicated.

The principles underlying the data processing itself include designating the specific person or persons responsible for handling access requests, and clearing

the procedures to be followed in the event of such requests. It is important to appoint a data protection coordinator in the company and to verify data compliance. He or she should also be able to provide answers in the event of questions about the legitimacy of the inclusion of specific data when the customer expresses doubt as to the need for such a wide range of information that the accounting office expects about him or her. In addition, rules should be drawn up for the formal revision of data by the coordinator, and other staff should be made aware of the coordinator's role and the need for cooperation with them. It is also important that those whose data are collected and processed are aware of this fact without raising unnecessary suspicion.

From the point of view of the use of data collection systems, it is important to adopt procedures to clear databases from unnecessary, outdated or customer-related data when the purpose for which they were collected has been achieved. It is also important to check the correctness of the maintained data, including their timeliness, with particular emphasis on sensitive data.

In the context of the measures for the protection of personal data, it is necessary to mention the protection of access to data only for authorized persons and at the same time to prevent unauthorized access. This applies to staff training as well as to the use of computer hardware and other physical security measures.

In the case of the accounting office staff, they should be familiar with the regulations of the GDPR, securing data in the IT system and the obligation of confidentiality. From the point of view of the equipment used, one should analyze server security, the use of wireless desktops, business computers in a local network or connected to the Internet, for example, used a LAN, MAN, etc., followed by an analysis of whether it is a private, protected or public network. In addition, there are important network protection systems, antiviruses, and anti-spyware. Computers should be password protected, passwords often changed and sometimes encrypted. One can also use automatic logout in case of interruptions.

Data entrustment agreements should also include clauses on the acceptance of the persons to whom the data will be 'sub-contracted' (e.g. an office to a company providing IT services), the possibility of controlling or inspecting the accounting office, the determination of the time − usually very short − within which the customer is to be notified of a possible incident of a personal data breach, and other measures to promote the security of data collection, processing and storage [https://www.rp.pl].

E. Szczepankiewicz conducted some research into ways of securing IT resources in Polish business entities and pointed to two hypotheses which she later confirmed, namely that the level of IT security of accounting resources in different groups of entities may differ significantly, although all entities should apply the requirements of the Accounting Act in the same way. She also determined that, in this respect, the differences identified may be due to the impact of additional sector-specific regulations and due the fact that in the private sector, only accounting offices and

audit firms comply more stringently than other small and medium-sized enterprises with the rules on the security of IT resources. It also stressed that theoretical models should be developed to enable effective methods and tools to be applied and appropriate legislative initiatives to be taken [Szczepankiewicz 2018].

Regarding the physical security features, it is worth mentioning the place of storing computers and documents kept in a paper version. It will be important to protect the access to the rooms from unauthorized persons, so the rooms should be locked with a key. This also applies to the cabinets used in them. In the case of documents which need to be destroyed, an office shredder should be used. For full security, the accounting office should also be equipped with fire-fighting measures such as smoke detectors and fire extinguishers. It is important for the company to appoint a person responsible for the security system used.

The above-mentioned methods of securing personal data do not exhaust the full scope of protection, but are to be the direction of actions that should be taken in the nearest future in accounting offices and other entities providing services within the broadly understood accounting. In particular, tax advisors and auditors should be mentioned here.

Therefore, as mentioned above, the entities to which the new rules apply also include advisory firms, including tax advisors and auditors. GDPR does not provide exemptions in this regard. On this basis, Resolution No. 93/2018 V National Council of Tax Advisers of 14 January 2018 on the authority of the National Council of Tax Consultants in the development, approval and adoption of the Approved Code of Practice of the National Chamber of Tax Advisors on the protection of personal data was introduced[2]. At the same time, the National Council of Tax Advisers was obliged to carry out information activities in a manner ensuring that the members of the Chamber adjust the provisions of the Code of Conduct until 25 May 2018, and appointed the Council to develop a Code of Conduct (KIDP) with regard to personal data. The effect of the activities in this area is the booklet prepared for the informant of tax advisors, *Ochrona danych osobowych przez doradcę podatkowego po wejściu w życie RODO* (*The protection of personal data by tax advisors after the introduction of GDPR*) which includes:

a) information on the processing of data in terms of the GDPR,

b) a description of key information obligations and personal data security, to which tax advisors will be obliged to comply,

c) specimens of statements and documents adapted to the specificity of the tax adviser's activity [Booklet 2018].

A similar situation also applies to the activities of auditors who, for the purposes of financial statements, use information from audited entities, where data controllers own the data. In order to ensure the protection of personal data, the State Chamber

[2] Resolution No. 93/2018 V National Congress of Tax Advisers of 14 January 2018. On the authority of the National Council of Tax Consultants for the development, approval and adoption of the Approved Code of Practice of the National Chamber of Tax Advisors on the protection of personal data.

of Statutory Auditors (PIBR) issued a relevant Note 36/2018 in which it included three annexes relating to this issue:

a) a specimen audit contract, which may apply to future contracts, including provisions on the rights and obligations of the parties to the contract arising from the GDPR,

b) a specimen of an entrustment agreement that may apply to ongoing audit contracts,

c) guidelines for an exemplary study contract and an exemplary entrustment agreement with regard to the provisions concerning the processing of personal data.

The purpose of the Note is to support the activities of the auditors by, inter alia, developing a sample audit agreement, as set out in Annex 1. In the opinion of the National Council of Statutory Auditors (KRBR), this agreement should be treated only as a proposal to be used, as the Civil Code expresses the principle of "freedom of contract" without imposing their final content and form. Thus, each contract concluded should be adjusted to the specificity and conditions of the order received by the auditor and also take into account the requirements of the National Audit Standard (KSB) 210, which are[3]:

a) the purpose and scope of the study,

b) the responsibility of the statutory auditor,

c) management responsibility,

d) an indication of the applicable financial reporting framework assumptions used in the preparation of financial statements,

e) a reference to the expected form and content of any reports to be issued by the statutory auditor and a statement that there may be circumstances that may cause the report to differ from the expected form and content.

The sample agreement also includes issues related to the rights and obligations of the parties to the agreements resulting from the implementation of the obligations of the GDPR, in particular with regard to newly concluded agreements.

The second Annex shows the principles favoring the application of the GDPR in already concluded contracts. They are organized by model (example) agreement for "Entrusting personal data". It may be concluded as a separate (supplementary) agreement from the audit agreement, regulating the processing of personal data. Moreover, the KRBR stressed that there is no need to conclude such agreements in relation to orders already completed.

Annex 3 to this Note contains detailed guidelines to complement the sample agreement and the sample entrustment agreement with regard to the provisions concerning the processing of personal data [Komunikat nr 36/2018…].

Violation of the GDPR has significant financial consequences. If the entity obliged to protect personal data is in breach, the entrepreneur has 72 hours to report

[3] Currently, following the implementation of the MSB, KSB 210 includes the provisions concerning KSRF (National Standard on Auditing) 210 Agreeing on the terms of the audit engagement, which refers to the auditor's liability for agreeing on the terms of the audit engagement with the management (and − if justified − the persons responsible for supervision), i.e. the audit agreement [www.pibr.org.pl].

the breach to the Office of Personal Data Protection − UODO (formerly GIODO). During the analysis and qualification of a specific violation, the effects that it may have on the individual(s) by undermining his or her (their) personal freedom shall be assessed [https://pomoc.mojebiuro24.pl]. On this basis, a financial penalty is charged, which involves an amount of up to 20 million or 4% of the annual worldwide turnover of the company, whichever is the higher.

4. Conclusions

The issue of protection of information and personal data has been known for many years, but has never before been the subject of such protection. Today's situation is a result of, among other things, the globalization of the economy and, consequently, the flow of data with the use of the latest technologies. Protecting sensitive data by those responsible, who undoubtedly include the professionals connected with business bookkeeping.

The conclusion formulated against the background of these considerations is that the problem of personal data protection has been taken up widely among institutions and service providers in the field of accounting (including consultancy and audit), which indicates an understanding of the need for personal data protection in the modern economy. This confirms the hypothesis that the passage of time has a significant impact on the understanding of the need to implement GDPR solutions.

Therefore, one can also point to the link between the behavioral accounting approach, where the behavior of decision-makers and persons performing certain tasks is analyzed, and the information generated by accounting and its procedures [Artieniewicz 2013].

Submitting a statement that the accounting office meets the requirements of the GDPR, in many cases becomes the basis for concluding a contract with the customer, and at the same time, the failure to comply with the recommendations of the Act in this respect may result in the risk of a fine being imposed by a supervisory authority and may lead to the loss of both current and future customers. The author's significant contribution to the research issue is the presentation of the key points of agreements (and discussion of their terms) that should be brought to the attention of parties in order to avoid misunderstandings and additionally, the way in which they should be implemented in order to adapt to the different actors in the field of accounting. The article may also be helpful in developing new contracts or correcting existing ones. The analysis of the existing regulations and the conclusions drawn from it will allow for proper the implementation of new solutions. This results from the author's research that the correct implementation of the GDPR solutions is therefore no longer seen as an additional complication and obligation, threatened with penalties in the event of non-compliance, but particularly as an opportunity to gain additional customers by assuring them of the complete reliability of the service provider with regard to the data entrusted to them.

References

Artieniewicz N., 2013, *Rachunkowość behawioralna jako interdyscyplinarny nurt rachunkowości i społecznych nauk o zachowaniu*, Zeszyty Teoretyczne Rachunkowości, t. 71 (127), SKwP, Warszawa, pp. 7-23.

Artieniewicz N., 2018, *Rachunkowość behavioralna*, CeDeWu, Warszawa.

Birnberg J.G., Shields J.F., 1989, *Three decades of behavioral accounting research. A search for order,* Behavioral Research in Accounting, vol. 1, pp. 23-74.

Booklet, 2018, *Ochrona danych osobowych przez doradcę podatkowego po wejściu w życie RODO,* prepared by the Commission on the drafting of the Code of Conduct of the National Chamber of Tax Advisers in the field of personal data, Warsaw, April 20.

https://pomoc.mojebiuro24.pl/-rodo-w-biurze-rachunkowym-jak-sie-przygotowac (accessed 10.11.2018).

https://www.rp.pl/Rachunkowosc/305099990-RODO-obowiazki-biur-rachunkowych-jako-administratorow-danych-osobowych.html (accessed 10.11.2018).

Jaworska E., 2014, *Perspektywa behawioralna w rachunkowości w świetle wybranych teorii psychologii motywacji,* Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 830, Finanse, Rynki Finansowe, Ubezpieczenia nr 70, pp. 49-58.

Komunikat nr 36/2018 Krajowej Rady Biegłych Rewidentów z dnia 5 czerwca 2018 r. w sprawie przyjęcia przykładowej umowy o przeprowadzenie badania ustawowego sprawozdania finansowego.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Resolution No. 93/2018 V National Congress of Tax Advisers of 14 January 2018 On the authority of the National Council of Tax Consultants in the development, approval and adoption of the Approved Code of Practice of the National Chamber of Tax Advisors on the protection of personal data.

Szczepankiewicz E.I., 2018, *Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach – wyniki badań*, Zeszyty Teoretyczne Rachunkowości, nr 97(153), pp. 115-138.

Szpytko-Waszczyszyn E., 2017, *Umowa powierzenia przetwarzania danych osobowych w biurze rachunkowym,* https://poradnikprzedsiebiorcy.pl/-umowa-powierzenia-przetwarzania-danych-osobowych-w-biurze-rachunkowym (accessed 16.05.2018).

The Act of 10 May 2018 on Personal Data Protection, 2018 (Journal of Law 2018, item 1000).

Trzpioła K., 2018, *RODO w księgowości i w biurze rachunkowym – sprawdź, jak przygotować się na nowe przepisy*, https://www.portalfk.pl (accessed 16.05.2018).

www.pibr.org.pl (accessed 14.06.2018).

OCHRONA DANYCH OSOBOWYCH W SYSTEMIE WSPÓŁCZESNEJ RACHUNKOWOŚCI W KONTEKŚCIE IMPLEMENTACJI ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 Z DNIA 27 KWIETNIA 2016

Streszczenie: Artykuł jest próbą analizy obowiązujących rozwiązań w zakresie ochrony danych osobowych. Analizie poddano materiały szkoleniowe oraz doradcze przygotowane na wskazany temat przez liczne kancelarie prawne (32) służące pomocą w prawidłowym wyjaśnieniu, zrozumieniu i we wdrażaniu nowo wprowadzanych obowiązków w zakresie ochrony danych osobowych. Autorka przeprowadziła pilotażowe wywiady w biurach rachunkowych (17) dotyczące ochrony danych osobowych, mające wskazać na podejście usługodawców do zadań z zakresu ochrony danych osobowych. Wśród kluczowych ustaleń będących pochodną prowadzonych badań zauważalny jest wzrost zainteresowania stron zawieranych umów zagadnieniami ochrony danych, a także prezentacja ich atutów oraz ewentualnych problemów w zastosowaniu w praktyce. Istotnym wkładem autorki w omawiane zagadnienie jest także prezentacja kluczowych punktów umów, na które powinny zwrócić uwagę strony w celu uniknięcia nieporozumień.

Słowa kluczowe: rachunkowość, usługi księgowe, ochrona danych, zachowania usługodawców,