SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIES NO. 145

SECURITY OF ACCOUNTING RECORDS IN THE UNITS OF A MUNICIPAL GOVERNMENT

Anna ĆWIĄKAŁA-MAŁYS[1]*, Małgorzata DURBAJŁO-MROWIEC[2]

[1] The University of Wrocław; anna.cwiakala-malys@uwr.edu.pl, ORCID: 0000-0001-9812-2118
[2] The University of Wrocław; malgorzata.durbajlo-mrowiec@uwr.edu.pl, ORCID: 0000-0003-0977-0960
* Correspondence author

Purpose: The aim of this publication is to diagnose if and to what extent the changes in personal data security were transferred to security of information/ data in terms of accountancy in the units of local self-government. Units of local self-government exploit more and more IT, they process more information, including personal data, and the number of users of such systems is growing. When we additionally take into consideration common accessibility to the Internet, with a growing number of devices and mobile applications and a growing number of cyber-attacks, then the needs of self-government for better solutions in terms of information security should be growing. Hence, following the May Regulation of the European Union, in terms of securing personal data, should conduce to implementing additional, safer solutions. Financial data is a particularly comprehensive set of information that is transmitted in the area of accountancy of units, including units of local self-government. In the area of accountancy, there is a special regulation concerning the security of data systems, more precisely it is the Accounting Act.
Design/methodology/approach: For the needs of this article, the researches were conducted in three average units of local self-government in the Lower Silesia Province. Interviews, observations and audits were also undertaken. In order to address this issue, interviews and audits were conducted in three units of local self-government of Lower Silesia Province.
Findings: It was determined that none of the researched units has and plans to create a complex system of security that is adequate to the existing risks.
Originality/value: The information security system in accounting was assessed, the area omitted in publications and practice.

Keywords: accounting, the security of information, personal data security, accounting policy.

Category of the paper: research paper.

1. Introduction

Units of local self-government, as with a majority of other units, exploit more and more IT systems with a more complex structure. They process more information, including personal

data, and the number of users of such systems is growing. The number, type and size of networks used are also growing (outside, mobile, wireless). The units use, to a great extent, remote transmission services and electronic transactions. When we additionally take into consideration common accessibility to the Internet, with a growing number of devices and mobile applications and a growing number of cyber-attacks, then the needs of self-government for better solutions in terms of information security should be growing. Hence, following the May Regulation of the European Union, in terms of securing personal data, should conduce to implementing additional, safer solutions.

Financial data is a particularly comprehensive set of information that is transmitted in the area of accountancy of units, including units of local self-government. In the area of accountancy, there is a special regulation concerning the security of data systems, more precisely it is the Accounting Act.

The aim of this publication is to diagnose if and to what extent the changes in personal data security were transferred to security of information/ data in terms of accountancy in the units of local self-government.

For the needs of this article, the researches were conducted in three average units of local self-government in the Lower Silesia Province. Interviews, observations and audits were also undertaken.

2. Legal basis for financial information security of local self-government

In the basic Legal Act that regulates managing the accountancy, additionally, in units of local self-government, more precisely in the Accounting Act (The Act on accounting, 1994), in chapter 8, the rules of security of bookkeeping vouchers, inventory documents, financial books and financial reports are specified (art. 71 of the Accounting Act) and all requirements in terms of keeping the database are laid-out (art. 73-75 of the Accounting Act).

In Art. 10(1) of the Accounting Act, it was stated that a unit should have documentation that defines all the rules of accountancy that were accepted – the so-called accounting policy. The last requirement from a legislator in Art. 10(1) of the Accounting Act, with reference to accounting policy, is an obligation to define a system that secures an information database. Additionally, Art. 10(1) para. 4 of the Accounting Act sets out with the usage of financial books, program rules of data security, including methods of securing access to data and to the computer system.

According to P. Walczak, units in the researched period should describe the security of the room in which data is processed and the security of IT stock and bookkeeping vouchers. Therein, attention is particularly focused on the security of bookkeeping vouchers because of the obligation to maintain the protection of personal data, tax or professional secrecy. Moreover, data security should be continuously enforced because one of the financial-accounting system

modules can be archiving at any one time. In rules covering security, it must also be stated when archiving is taking place, e.g. at the end of the month and in which way, e.g. by saving data on media and determining a safe place for keeping (Walczak, 2018).

According to A. Hołda, the accounting rules that are to be followed by a unit should define: 'technical-organizational ways of keeping the accounting books and their security' (Hołda, 2018). Security of accountancy is clearly addressed in the following regulations and acts:

- Regulation of the European Parliament and of the Council (EU) 2016/679 of 27th April 2016 on security of legal person due to personal data processing and free flow of such data and setting aside the directive 95/46/EC (general regulation on data security)[1],
- Regulation of the Council of Ministers on Legal Framework of Interoperability, minimal requirements for public registers and exchange of information in an electronic form and minimal requirements for computerized systems (ICT),
- The Act of 6th September 2001 on access to public information.

In the general regulation on security of personal data, the rules for processing personal data are defined, including the requirements that must be fulfilled by a unit of a local self-government as an administrator of an extensive collection of data, including people that submit payments to the municipality, so the data that is included in the accounting books.

In paragraph 20(1) of the Legal Framework of Interoperability, the units that are in charge of public activities are obliged to develop, implement, exploit, monitor, maintain and improve a management system of information security. In the next paragraph the most vital actions that need to be taken by a unit as to ensure confidentiality, accessibility and integrity of information are defined. In article 3 of this paragraph it was stated that when a management system of information security in a unit is certified by PN-ISO/IEC 27001, then it is considered that the demands from Legal Framework of Interoperability are fulfilled.

In the Act on accessibility to public information, it was indicated that every single item regarding public issues of information should be accessible in the Bulletin of Public Information or at the request of an interested person. The majority of public cases are recognized in the financial dimension so it is reflected in accounting records[2].

3. Implementation of documentation duties

The researched units of a local self-government fulfilled to various extent, their duties according to the act on accountancy in the area of accountancy policy. In Table 1,

[1] More information on personal data protection can be found in M. Durbajło-Mrowiec (2018).
[2] Due to limited space, the influence of other legislation acts on accounting information in detail was not discussed.

the questionnaire of consistency of accepted rules of accountancy according to legal requirements in the three units under research are revealed.

Table 1.
Questionnaire of consistency of financial policy in the researched municipal government units

Item no.	Specification	Unit A		Unit B		Unit C	
		YES	NO	YES	NO	YES	NO
1.	Has the unit defined if it is resilient to risks from data storage (art. 71(2) of the Accounting Act)?		x	x			x
2.	Has the unit adjusted its external protective measures (art. 71(2) of the Accounting Act)?		x	x			x
3.	Has the unit defined the rules of making spare copies from stored data on the IT database, assuming sustainability of data storage (art. 71(2) of the Accounting Act)?		x	x			x
4.	Has the unit defined protective measures for securing computer programs and IT accounting system data by using the appropriate program and organizational solutions that protect the data from unauthorized access or damage (art. 71(2)2 of the Accounting Act)?		x	x - a system of ID is in place, - authorizing passwords are required, - training for data security provided for employees, - firewall equipment ensures logical protection and is provided, - servers are located in designated rooms with access only for authorized employees, - maintenance is undertaken according to the recommendations of the supplier and by an authorized person, - the server and the computer are protected by anti-virus software, - the head of the unit decides who is authorized to access the system		x - a system of ID is in place, - authorizing passwords are required, - firewall protection on internet connections is provided, - the server and the computer is protected by anti-virus software, -a policy of authorization is practiced in the system	

Cont. table 1.

5.	Has the unit defined the kind of medium of information for storing data with specified durability from the point of view of binding time of archiving?		x	x - on electronic media on a weekly and on a monthly basis, - 2 weeks copies are stored for a month, monthly copies are stored for six months, - paper or disc copies are stored in a fireproof armored cabinet by an authorized IT employee, - collections in the system are stored incrementally and archived for 5 years, - collections of data on the server are protected by the mirroring of drives – parallel record on two drives, one of which serves as a backup.		x - monthly backups are stored until the capacity of the drive is reached,	
6.	Has the unit defined its obligation to make backups for collections of data?		x	x			x
7.	Has the unit specified rules for protecting computer programs and collections of data (against unauthorized access or damage)?		x	x			x
8.	Has the way of gathering data been defined (art. 73(1) the Accounting Act):		x				x
	- in the original version,				x		
	- in a specified manner adjusted to the process of keeping the accounting books,			x			
	- as divided into reporting periods,				x		
	- in a way that allows for easy access for authorized persons,			x			
	- per annual collections of bookkeeping vouchers and inventory documents which are labeled appropriately with final dates and final numbers of the collection?				x		
9.	Has the place of storing data been defined (art. 73(1) the Accountancy Act)?		x	x			x

Cont. table 1.

10.	Has the possibility of moving the content of bookkeeping vouchers to IT media been enacted so as to allow it to be kept permanently and unchanged until when devices for displaying the content and print versions are available (art. 73 (2) the Accounting Act)		x		x		x
11.	Has the time for storing been defined) (art. 74 the Accounting Act?		x	x			
12.	Has the rules for sharing the collections of data or their parts with a third person been defined (art. 75 of the Accounting Act):		x				x
	- with the consent of the manager of the unit or an authorized person if sharing is within the unit,				x		
	- outside the unit – with the written consent of a manager and with a record of taken documents?			x access is given only for law enforcement authorities or courts			
	Have the rules for storing in case of terminating the business been defined? (art. 76 of the Accounting Act):		x		x		x
	- as a result of joining with another unit or changing a legal form – storing is on the continuing unit side,						
	- when the tax units were liquidated either as a designated unit or a person and the storing unit is informed by the manager, liquidator, trustee, is the information passed to a court or any other unit that keeps the record of business activities or to a treasury office?						
13.	Have any additional procedures been enacted? If yes, please give which.			'Every employee is responsible for the documents that are being accessed or held at his working place. Rules for transferring acts to the archive are as stated, e.g. at the end of the case and on the basis of an acceptance report' Bookkeeping vouchers that were registered cannot be transferred from the Financial Division		In terms of balance policy, there is an obligatory element for data protection but further parts of this policy are not extended.	

Cont. table 1.

14.	Have any changes been introduced in the accounting policy regarding accounting data security after 25th May 2018, after introducing the regulation on data security?		x		x		x

Source: Self-study on the basis of an audit of accounting policies and Chapter 8 of the Accounting Act.

As it can be seen, unit A had not addressed the problem of data and its collection protection and did not utilize a secure IT system for information processing regarding accountancy.

With regard to unit B, this had in place a policy of information security that distinguished procedures on archiving the accounting documents and the rules of creating, storing and archiving financial-accounting documents. In addition, the categories of archive documents are defined and rules of storing the acts are specified. With regard to creating, storing and archiving financial-accounting documents, information was made available about the practices on grouping documents, completing documents, labeling documents in order to easily find them, labeling the acts, unit storage and working place storage, as well as individual responsibility of employees for documents that are gathered at their working place. Moreover, a policy exists for secure waste management. Furthermore, in the rules of storage, there are also:

- Rules on file description: according to registering instruction.
- Procedures for working place and facility archive.
- Information on time of storing: up to a year at working place except for documentation that is necessary for further execution of duties, the latter can be stored at a working place up to 5 years.
- Rules on transferring the acts to a facility archive: only full-year registers on the basis of an acceptance register are allowed, after previous ordering and agreement with a responsible employee.
- Rules on storing acts in the archive: that maintenance is undertaken every five years and acts with special meaning are stored under specific procedures
- Rules on sharing accounting documents: inside the unit – only with the authorized entities within the financial department, without the possibility to share documents with external units such as law enforcement authority, unless with a court order or the written consent of a Mayor, against receipt.

Additionally, in the description of the applied data processing system, there are rules about IT data security wherein physical and logical security is provided, an up-to-date firewall system is utilized, servers can only be exploited in designated and protected rooms, that maintenance is upheld according to supplier recommendations, anti-virus programs used for protecting servers and computers are current, rooms having limited access and the system is accessible only by authorized employees, a system of assigning authorization and passwords is in place, that administrator of the system is designated and rules of archiving data on electronic media are applied that involve making weekly copies and where the data is closed after a month and is archived in the system for five years only.

In spite of mentioning the many elements required, art. 72-75 of the Accounting Act, the way of gathering data was not specified (art. 73(1) of the Accounting Act). What is more, proceedings with financial documentations in case of terminating a business activity were not stated (art. 76 of the Accounting Act).

In none of the researched units were changes made to be compliant with the common regulation on data protection of 25th May 2018.

4. Applying rules and methods of accounting information security in researched units

In the Accounting Act, but also in the Legal Framework of Interoperability, in a general regulation on personal data protection, public units are obliged to create and maintain systems of information security. In each of the mentioned legal regulations the legislator demands entities that process information apply identical or very similar protection. In Table 2, a questionnaire of consistency of information protection systems in the researched units is presented in terms of accounting information.

Table 2.
A questionnaire of consistency of rules and methods used to protect accounting information

Item no.	Specification	Unit A		Unit B		Unit C	
		YES	NO	YES	NO	YES	NO
1.	Are departments of accounting and server areas of processing designated?		x no areas were determined		x no areas were determined		x no areas were determined
2.	Have accounting employees been authorized to process data?	x		x		x	
3.	Have employees signed declarations on keeping the secrecy of information gathered at work?	x		x		x	

Cont. table 2.

4.	Have employees been trained in the area of personal data protection	x			x not all managers have spoken to their employees		x they are gradually being trained
5.	Does a unit make backups of accounting data?	x		x		x	
6.	Are computers utilized in the accounting department protected against unauthorized access:						
	- by password		x	x		x	
	- by anti-virus software	x		x		x	
	- by screensaver?		x		x	x	
7.	Is access to the financial-accounting program protected:						
	- ID and access password enacted		x	x		x	
	- automatic logout of device enacted after a set time period?		x		x		x
8.	Have there been any cases of transferring passwords?			x many people have it written down in well known places		x they are known by many employees	
9.	Are the screens reversed from the entrance door?		x can be viewed	x		x a majority of them	

Cont. table 2.

10.	Are the computers switched off after finishing the work day?	x		x there are fa ew cases when the computers were left switched on		x they are not switched off from the safety bar	
11.	Have the working places been controlled after finishing work in the last half of the year?		x	x			x
12.	Have any documents been left on the desk after finishing the day's work?		x		x		x
13.	Is only necessary documentati on on the desk during the work?		X Not always	x rather yes			x rather not
14.	Can the documents on the desks be seen by unauthorize d people		x		x		x such situations can happen
15.	Are pieces of paper used on one side and used on the other as well?	x occasion-nally		x due to saving		x occasionally	
16.	Do employees use portable tools such as pen drives, laptops?		x accounting division employees cannot bring in personal laptops		x		x there is no option to connect pen drives
17.	Is the server used for transferring accounting data in a separate room?	x		x		x	

Cont. table 2.

18.	Is the room air-conditioned?		x		x		x
19.	Are computers and server protected against voltage drop?	x UPS		x UPS		x UPS	
20.	Are there additional devices plugged in the bar that is designated for computers (e.g. heaters, kettles, fans)?	x not enough sockets are available in the workplace		x the building is from the 50-ties, not many sockets are placed in comfortable locations. Devices are used that may cause a short circuit (kettles).		x may happen, there is ban on using heaters	
21.	Has the unit defined the kind of information media used to store data?	x on electronic media		x on electronic media		x on electronic media	
22.	Are backups used?	x		x		x	
23.	Are the backups stored by the IT employees of the unit?	x		x		x	
24.	Are firewall tool used?	x these were purchased		x		x	
25.	Have the rules for gathering and ordering files been changed, as well as rules for sharing accounting documents so as to be compliant with current law?		x used according to art. 73(1) of the Accounting Act)		x used according to art. 73(1) of the Accounting Act)	x an obligation is followed to keep receipts when sharing the collections	x

Cont. table 2.

26.	Are accounting documents stored outside the department?		x	x in a handy storage			x
27.	Are conservative actions and repairs of computer devices and servers conducted under the supervision of IT employees of the unit?	x if they are conducted in the unit		x in case of maintenanc e work outside the unit, the data is deleted from the devices		x	
28.	Is data deleted from computers that are transferred to schools?	x		x		x	
29.	Is a remote desktop used for eliminating mistakes in software application?	x		x		x	
30.	Have there been any unencrypted collections of data send to technicians?		x	x			x
31.	Is there any confidentiali ty clause or additional agreement with technicians of the financial-accounting systems?		x only for processing personal data		x only for processing personal data		x

Cont. table 2.

32.	Is the content of accounting documents transferred to IT media (art. 73(2) of the Accounting Act)?		x		x there is a plan to buy new software which will give such possibility		x
33.	Are the acts transferred to the archive after finishing procedures?		x not always		x they are transferred when the surface of the archive is released	x in most of the cases	
34.	Are the acts transferred to the archive prepared by employees in charge of the case?		x transfer is by a designated person	x			x by a person that is not so overloaded with work
35.	Is the transfer of the act registered?		x	x		x	
36.	Is there a possibility for employees to interfere with the software of devices?	x new servers have been installed that enable such practice		x inventory of computers in progress		x employees of the promotion division utilize private, specialized software	
37.	Are used CDs destroyed?	x in shredders		x by IT employees			x there is no procedure for doing so
38.	Have competences of the IT systems been recently verified?		x	x		x final changes have not been implemented yet	

Cont. table 2.

39.	Can employees copy accounting data, including coping on paper?	x there is an obligation to destroy a copy when it is not vital		x downloading can only be of the data necessary to fulfill the work		x regarding supplementary material at work, the obligation is to keep data in files until the work is done and then it must be destroyed	
40.	Are the files with data stored in locked cabinets?	x some of them are on shelves without secure access		x some are stored outside the cabinets			x storage depends on the possibilities
41.	Are the keys to rooms and cabinets secured after finishing the work?		x key to cabinets stay in place		x employees take the keys with them	x keys to cabinets and shelves are kept in one place and keys to rooms are left with security workers	
42.	Are the rooms cleaned in the presence of employees?		x in the afternoon		x in the afternoon, according to work regulation		x parts of strategic rooms such as the Mayor's office or the treasurer's, the secretary's or the auditor's cleaning is done during working hours
43.	Have there been any cases of disclosure of accounting data?		x	x a few times			x

Cont. table 2.

44.	Are there any cryptographic ways of securing data?		x the possibilities are integrated within the financial-accounting system and are not identified		x		x there is no need
45.	What kind of specific protective means are used in accountancy?	- written declaration on keeping treasury secrecy, - obligation to attend ethics department briefings - proper choice of employees.		- few bank accounts with an adequate division of responsibilities, - written declaration on keeping treasury secrecy - obligation to attend ethics department briefings - introduction of hierarchical authorizations - e.g. only managers are entitled to share information with other internal units, while information sharing with external units is only possible for the accounting officer and treasurer, - allocating all unit employees workplaces in connected rooms isolated from other departments, - direct supervision of the treasurer is applied, - strict rules of working introduced by the accounting officer, - significant overloading with work.		- division of bank accounts and limitation of access to chosen employees, - written declaration on keeping treasury secrecy - introduction of an ethic code, - introduction of limitations in accounting information transfer to people outside the accounting department, providing accounting documents to employees, moving documents to other buildings.	

Source: self-study on the basis of conducted interviews, observations and the Accounting Act, Legal Framework of Operability and general regulation on the data protection.

The results of conducted researches confirm the inefficiency of securing systems of accounting information. In the presented questionnaire there are questions about basic means of information protection. It appears that even at this level the analyzed units do not comply with the requirements, e.g. they do not use or improperly protect access passwords, carelessly use workstations and screens, do not systematically transfer files to archive, can change the configuration of computers, they can install their own software and inadequately secure their cabinets and rooms. Amid the analyzed units, there is one that stands out. Here, awareness of information protection is higher than in the others. In this unit, there was an expert employed to order the area of personal data protection until a general regulation on personal data protection was put in place. In the remaining two units, the functions of Administrator of Information Security were performed by employees of the units in combination with the

function of an administrator with other duties. Entrusting this function to an external expert, creating and implementing a system of personal data protection brings about the implementation of protective mechanisms for all information, not only the data of a legal person. In this unit, establishment of secure means of protecting data were continued after the 25th May 2018. As a result: new authorizations were given in the financial-accounting system and written applications were introduced to issue authorization to process data and to work upon the system. Moreover, employees met with ongoing discussions on data protection, cybercrime and rules of procedure. In addition, accounting department employees signed obligations to keep the secrecy of information gathered during their work, and protective tools were installed. In the remaining two units, no vital changes were introduced with regards to accounting information protection or to meet general regulations on data protection.

A huge threat to the protection of accounting information in the two units is that the financial-accounting system that is utilized has been exploited for over five years without major modifications being introduced. Of note only one of the analyzed units budgeted in 2019 for updating and installing new financial software.

5. Conclusions

Summing up, it should be stated that none of the analyzed units possess and plan to create a complex protection system adequate to the existing threats. Such a protection system should be composed of personal data protection, security of information according to PN-ISO/IEC 27 000 norm, IT protection, awareness of the employees and securing continuation of actions. As is evident, implementing European Union regulation did not have an effect on financial data protection in the analyzed units of local self-government. This is due to little interest in managing a team of such units with regards to system protection of information, limited financial sources, underestimation by voters of such invisible actions (other than completed investments), lack of severe sanctions in the existing legislation and inefficient execution of the law.

References

1. Act on 29 September 1994, on accounting, Journal of Laws (2018).
2. Act on 6 September 2001 r. on an access to public information. Journal of Laws (2018).
3. Durbajło-Mrowiec M. (2018). Ochrona danych osobowych w rachunkowości. *Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego*, *Finanse i Rachunkowość, 4*. doi:10.23734/23.18.010.
4. Hołda A. (2018). *Instrukcje księgowe i podatkowe.* Retrieved from https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damjzhaztanq, 23.10.2019.
5. Regulation of the Council of Ministers of 12 April 2012 on Legal Framework of Interoperability, minimal requirements for public records and exchange of information in an electronic form and with minimal requirements for ICT systems, Journal of Laws (2017).
6. Regulation of the European Parliament and the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regards to personal data processing and with regards to free flow of such data and repealing directive 95/46/EC (general regulation on data protection), Official Journal (2016).
7. Walczak P. (2018). *Dokumentacja wewnętrzna w jednostkach sektora finansów publicznych.* Retrieved from https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3damrqge4tcoa, 23.10.2019.