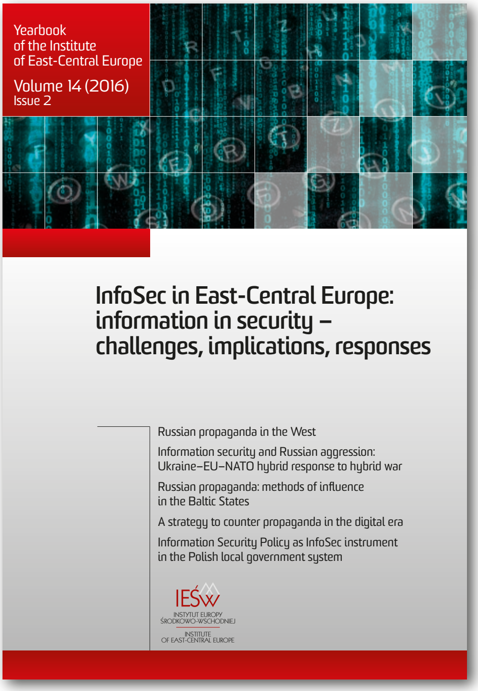

Yearbook
of the Institute
of East-Central Europe

Volume 14 (2016)
Issue 2

InfoSec in East-Central Europe: information in security – challenges, implications, responses

Russian propaganda in the West

Information security and Russian aggression: Ukraine–EU–NATO hybrid response to hybrid war

Russian propaganda: methods of influence in the Baltic States

A strategy to counter propaganda in the digital era

Information Security Policy as InfoSec instrument in the Polish local government system

IEŚW
INSTYTUT EUROPY ŚRODKOWO-WSCHODNIEJ
INSTITUTE OF EAST-CENTRAL EUROPE

Yearbook of the Institute of East-Central Europe
(Rocznik Instytutu Europy Środkowo-Wschodniej)

Publication details, including instructions for authors:
http://www.iesw.lublin.pl/rocznik/index.php

Information Security Policy as InfoSec instrument in the Polish local government system

Łukasz Wojciechowski[a]

[a] University of Economics and Innovation (WSEI), Lublin, Poland

Published online: 05 Dec 2016

To cite this article: Ł. Wojciechowski, 'Information Security Policy as InfoSec instrument in the Polish local government system', *Yearbook of the Institute of East-Central Europe*, vol. 14, no. 2, 2016, pp. 75-94.

Yearbook of the Institute of East-Central Europe, 2016, Vol. 14, No. 2, 75-94

Łukasz Wojciechowski

Information Security Policy as InfoSec instrument in the Polish local government system

Abstract: This article discusses Information Security Policy (ISP) as an instrument of maintaining information security (InfoSec) in Poland at the local government level. In line with the existing legal framework, all local government units must prepare and implement a document titled 'Information Security Policy' (ISP). Resulting from a landmark law, i.e. the Act on Personal Data Protection of 29 August 1997, the ISP determines the data sets, the range of their processing as well as basic mechanisms of their protection. Another important source of law in the field of InfoSec in Poland is a 2004 Regulation on Personal Data Processing Documentation (RMIA) that sets out details that apply to individual institutions and define the technical conditions of the equipment and systems used for the processing of personal data. That regulation proved fundamental for the development of contemporary InfoSec in Poland. Appropriate security policy in local government units may protect them from cyberattacks at various levels and hence provide Polish citizens with InfoSec. However, the introduction of appropriate procedures faces many challenges. They may result not only from the lack of qualifications on the part of officials processing the data but also from scarce financial resources necessary for the implementation of relevant procedures.

Keywords: Information Security Policy (ISP), information security (InfoSec), Polish territorial self-government, data processing, legal frameworks.

Introduction

Information security (InfoSec) is one of the most important areas of security at both domestic and international levels. For the sake of the clarity of the argument developed in this paper, the following definition of InfoSec will be employed: "InfoSec ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)."[1] The term 'enterprise' may be replaced by 'institution'[2]. The number of devices connected to the Internet in 2015 was estimated at 15 billion.[3] As a result, the number of threats in cyberspace increases regularly around the world, including Poland. One of the most important elements to ensure the security in this field is proper preparation of the local government administration.

At the beginning of the 1990s, the legislators in Poland intensified the work on the law on personal data protection. The complexity of the issue triggered a lively debate on new legal solutions. The Act on Personal Data Protection of 29 August 1997 (APDP) functions with amendments to this day. The next step in creating the conditions for InfoSec in Polish territorial self-government was to reform the whole local government system, including the three-tier division into communities, counties and voivodeships.[4] That new administrative structure entered into force on 1 January 1999. The final stage of the process aimed at establishing the legal framework conducive to the maintenance of InfoSec was the implementation of the Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 on Personal Data Processing Documentation, Technical and Organizational Conditions, which Should be Fulfilled by Devices and Computer Systems Used for Personal Data Processing (RMIA).[5]

The objective of this article is to examine the micro-level dimension of InfoSec and to discuss the ISP as a necessary tool that complements it. The author also verifies the hypothesis that InfoSec of all citizens depends largely on proper preparation and implementation of the internal regulations of individual institutions. Another

[1] ISACA, *Glossary of Terms*, Information Systems Audit and Control Association (ISACA), http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (2016-01-04).

[2] Referring to, among others, institutions of Polish territorial self-government.

[3] P. Pawlak, 'Governance of Safety and Security in Cyberspace', in: P. Dąbrowska-Kłosińska (ed.), *Global safety governance: Challenges and Solutions*, Centre for Europe, University of Warsaw, Warszawa: Aspra-Jr, Warszawa 2015, p. 205.

[4] Cf. J. Regulska, 'Governance or Self-governance in Poland? Benefits and Threats 20 Years Later', *International Journal of Politics, Culture & Society*, vol. 22, no. 4, 2012, pp. 537-542.

[5] The newly formed Polish territorial self-government was given real tools to deal with the issues of information security. One of the most important tools was the Information Security Policy which states the rules for creating the internal regulations in local government units and has become an essential InfoSec instrument in Polish territorial self-government. Despite many difficulties in the implementation of this instrument, it is worth emphasizing that the Polish authorities (e.g. various offices) played the major role in the revolution of InfoSec in Poland.

hypothesis refers to the major role of every single civil servant in InfoSec issues in Polish territorial self-government. The question is to what extent the changes which took place in the legal environment in Poland following 1989 have contributed to that. While focusing on the new technologies in the fight against cybercrime, one should remember that the responsibility for the security of citizens' personal data lies within the scope of an individual civil servant and his or her computer even in the smallest units of local self-government. What is more, the policy-makers emphasize cyber-sec and IT approaches to avert information-related threats to security. However, they tend to underestimate the actions which are cheap and easy to be implemented, but may in fact improve a country's resilience to InfoSec threats. In order to address the aforementioned points, the argument in this article is structured as follows. The first part examines the legal framework pertinent to personal data security in Poland and its influence on the office procedures in Poland. In the second part, the ISP is examined in detail and the most important aspects of its connection to InfoSec are highlighted. In the third part, the implementation of the ISP in Polish territorial self-government is discussed along with the description of different tiers and selected problems encountered in the implementation process.

1. The legal framework

1.1. The law on Personal Data Protection

The Polish Parliament adopted the law on Personal Data Protection on 27 August 1997. It should be highlighted that the law was a modern and forward-looking act. To this day some changes have been introduced, but most of the provisions have not changed and are still in force. The Act is the most important piece of legislation governing the information security of citizens and of state institutions. The ISP, which is the subject of this study, does not directly result from the Act, but it is a clear determinant for the territorial self-government with its elaboration and development of other documents related to information security. It is worth mentioning that the issue of responsibility is taken into account by the legislators. Additionally, it develops and precisely defines the concept of the Personal Data Administrator who automatically becomes the head of a state institution or a company. The boss must organize the work in his institution in a way that ensures the maximum level of InfoSec regardless of whether we are dealing with a hierarchical or horizontal structure.

The Act in the present shape consists of 9 chapters. In addition to the general provisions, transitional provisions and penalties, the legislators raise the following issues: personal data protection authority, rules for processing personal data, rights of persons whose data are processed, securing of personal data, reporting data set and information security administrators and transfer of personal data to a third country. The General Inspector for Personal Data Protection (GIPDP) is the data protection authority. The supporting institution is the Office of the General Inspector for Personal Data Protection. The GIPDP is appointed for a 4-year term by the Polish parliament. According to the Act, the most important tasks of the Inspector should be: to issue administrative decisions and to consider complaints with respect to the implementation of the rules on personal data protection, to keep the register of data sets, to give opinions on legal instruments relating to the protection of personal data, to monitor the compliance of data processing with the provisions of the Act, to initiate and undertake activities aiming at improving the protection of personal data, to participate in international organizations and institutions dealing with personal data protection.[6] The major position of the GIPDP who is given instruments to act is confirmed by the fact that since 19 September 2015 the GIPDP may not be, without the prior consent of the Sejm, held criminally responsible or deprived of freedom unless he or she agrees. Besides, the GIPDP cooperates with the parliament and submits an annual report on his or her activities.

The chapter describing the rules for processing personal data is a practical instruction for government and territorial self-government institutions as well as entrepreneurs on the basic rules of data processing. It is important that the closed catalogue was created referring to the situations where data processing takes place. The catalogue includes the following: the need for the consent of the person

[6] Act on Personal Data Protection of 29 August 1997, art. 12, *Journal of Laws*, 2014, item 1182 as amended.

whose data are processed, the need for stating the legal basis for data processing or justifying the data processing for the public good.[7] The completion of this chapter is constituted by another catalogue containing the rights of persons whose data are processed.[8]

The chapter focusing on securing personal data defines the possibility of assigning the Information Security Administrator who can only be a natural person, i.e. cannot be a company or have other legal forms. Furthermore, he or she acts as a supervisor under the authority of the Personal Data Administrator in compliance with the application of technical and organizational measures to ensure the protection of personal data processed in a manner appropriate to the risks and category of data being protected. The head of the institution decides whether or not to appoint an Administrator of Information Security. If he or she chooses not to appoint any employee for that function, he or she becomes automatically responsible for the obligations arising from this position. Due to progressing internationalization of trade, the legislator had taken into account the transmission of personal data to third countries, which was included in the Act. The term 'third countries' refers to countries from the non-European Economic Area and those indicated by the European Commission that guarantee an adequate level of protection.[9] The need for obtaining the consent of the GIPDP to transfer data to third countries (only in some cases) is an additional protection guarantee. Furthermore, it requires a form of an administrative decision.

1.2. The Regulation on Personal Data Processing Documentation (RMIA)

The legal instrument of the lower rank that gave the final shape to InfoSec for Polish authorities and companies is the RMIA. The regulation clarifies the directions which were given by the Constitution and APDP. The documentation is based on this regulation and the procedures are prepared and implemented in all offices and businesses. The

[7] Ibid., art. 23.

[8] This section clarifies the constitutional provisions described above and includes a detailed list of citizens' rights in the context of the changes, insights and deletion of their data.

[9] They guarantee an adequate level of protection required by art. 25 of the Council Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC).

regulation describes three areas. The first one is the way of conducting and the scope of documentation describing the way of personal data processing as well as technical and organizational measures used to ensure the protection of personal data processed appropriate to the risks and category of data being protected. The second one is basic, technical and organizational conditions that should be fulfilled by devices and computer systems used for personal data processing. The third one is the requirements for the record of disclosure of personal data and the security of personal data processing.[10]

The head of each institution or company is required to implement two documents. The first is the Information Security Policy. The second one which often functions as an appendix to the Information Security Policy is the IT System Management Instruction Used to Process Personal Data. The security policy includes in particular: 1) the list of buildings, premises or their parts comprising the area where personal data are processed; 2) the list of data sets with an indication of software used for data processing; 3) the description of the structure of data sets showing the contents of particular information fields and connections between them; 4) the way of data transfer between different systems; and 5) the definition of technical and organizational measures necessary to ensure the confidentiality, integrity and accountability of the processed data.[11]

The Instruction Used to Process Personal Data includes in particular: 1) the procedures for granting authorization to process data and the registration of such rights in the computer system and an indication of the person responsible for these activities; 2) the methods and means of authorization and procedures connected with their management and use; 3) the start, suspension and end of an employee's work in the system; 4) the procedures for backing up data files and programs and software tools for their processing; 5) the method, place and period of storage of electronic media and backup; 6) the way of antivirus protection; and 7) the procedures of executing the inspection and maintenance of systems and information media used for data

[10] Regulation on Personal Data Processing Documentation, Technical and Organizational Conditions, which Should be Fulfilled by Devices and Computer Systems Used for Personal Data Processing of 29 April 2004, art. 1, Journal of Laws, no. 100, 2004, item 1024.

[11] Ibid., art. 4.

processing.[12] This Regulation and annex precisely determine technical and organizational conditions that should be fulfilled by devices and computer systems. Their range depends on the data type and the form of their processing.[13]

2. The content of the Information Security Policy

2.1. Organization and infrastructure processing of personal data

Lawmakers provided only the general framework for the documentation which should be developed in every company and institution. The decision as to give managers the freedom in the development of the Information Security Policy was intentional and justified. The variety of entities in which the solutions worked out is considerable. Notably, the various institutions of local government differ from one another. That is why the heads of institutions who, in accordance with the law, were appointed Personal Data Administrators, are responsible for the creation of appropriate internal rules. The competent security of InfoSec issues needs to consider the documentation as a guideline understandable to employees at all levels. It should also be short and easy to understand for every employee who is authorized to process personal data.[14]

It is important to note that the Information Security Policy begins with a glossary of terms in which employees who are not familiar with law and IT could check the meaning of various terms. Then, the authors of the document can focus on the organization of the processing of personal data. In this section, the tasks and responsibilities assigned to all data processors are determined, starting from the Personal Data Administrator, followed by the reference to the Information Security

[12] Ibid., art. 5.

[13] Aware of the systematically increasing number of cyberspace criminal offences, the Minister decided that one of the most important criteria in determining the necessary degree of danger will be whether the computer is permanently connected to the Internet. If so, the requirements increase significantly. Taking into account that currently the majority of computers have such a connection, it can be concluded that the requirements for most Personal Data Administrators are restrictive.

[14] P. Fajgielski, *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony* [Information in public administration. Legal aspects of gathering, sharing and protection], Wrocław: PRESSCOM, 2007, p. 115.

Administrator (if he or she is not appointed, his or her responsibilities are automatically transferred to the Personal Data Administrator).[15] It is also necessary to explain the basic information security duties to all the other employees who process data. The duties include, for example, protecting the data against unauthorized access or processing personal data only to the extent permitted. Furthermore, an employee receives a unique identifier and a password for the processing of personal data in the computer system. To make the document comprehensive and adequate to the institution, the author also has to give a detailed description of the data processing infrastructure.

2.2. A list and description of the structure of personal data sets

In order to organize resources for their proper protection, Personal Data Administrators make a list of personal data sets. The preparation of such a list requires a review of all the activities of the institution and takes a lot of time. According to the GIPDP interpretation of the rules, the documentation must include all the files, even if they are not listed in the catalogue of the data sets which do not need to be registered. The development of this part of the documentation is much easier in the smallest units of self-government than in the largest offices. However, a group consisting of representatives of various departments may participate in drafting the list. If data sets are clearly defined, in case of a cyberattack the affected area can be effectively identified and disconnected from the rest.[16]

The next elaboration, which is much more detailed, is a description of the structure of personal data sets. It contains subsets that clarify the previously described list. For example, if there is a data set called 'Office employees', the description of personal data sets would be 'personnel files', 'employment contracts', 'social benefits fund' and 'employees' agreement to the processing of their data'. Furthermore,

[15] The following are the examples of his or her responsibilities: to check the compliance with the provisions on the protection of personal data, in particular by checking the compliance of personal data processing with the rules on personal data protection, and to write an annual report on this area. Separating both functions in the documentation is beneficial, even when the Information Security Administrator is absent but may occur in the future and will not need to make changes to the documentation.

[16] M. Kowalewski, J. Kowalewski, *Polityka bezpieczeństwa informacji w praktyce* [Information security policy in practice], Wrocław: Aspra-Jr, pp. 116-121.

a legal basis for the processing should be included. It means that each position needs to be supported with a legal act on the basis of which it is processed. In order to complete the list, the author must fill in the detailed structure of the set (stating which data elements are included in each set), re-determine how the data are processed (in the material or virtual form) and specify who is authorized to process them. If there is a large number of employees, there is no need to mention them by name, just to name a group of employees. If the data sets are processed in a computer, the names of data sets and the names of computer programs that are used to process them need to be assigned.

As far as large offices are concerned, it is also crucial to show the way of data transfer between individual computer systems. An accurate and precise computer network diagram and a detailed list of data sets help to prevent threats in cyberspace. The Information Security Administrator and IT System Administrator (if they are appointed) have a better overview of the security of data transfer due to the existence of the scheme. It also speeds up the process of eliminating the weakest points when necessary.

2.3. Specifying the technical and organizational measures

The most practical part of the Information Security Policy is called 'Specifying the technical and organizational measures'. Its preparation is an audit of all the items connected with the protection of data sets in the institution. Moreover, it is a part of the policy which is the most useful one for employees who are not familiar with law and IT. Depending on the specificity of the workplace, Personal Data Administrators can place there information concerning: the system of training and improving knowledge in the field of personal data protection, the confidentiality of data, the security of devices and the safety of a data storage device, the use of documents outside the headquarters, the system access control, disclosing personal information and the responsibilities of employees authorized to process the data, etc. At this point, the author elaborates on each of the aforementioned points.[17] Various aspects of InfoSec, with a particular

[17] Loc. cit.

emphasis on the protection of personal data, include a human resources policy at the stage of recruitment. Therefore, the Information Security Policy should include procedures related to the employee recruitment. Through appropriate procedures, one of the factors taken into account when applying for a job can be knowledge or an aptitude for InfoSec.[18]

The issues related to the security of devices and data storage include two areas. The first one is the protection against data loss. Employees may not realize that data backing up is important, but they should learn it with the use of the right procedures. The second area covers the protection of data from unauthorized access. This concerns both the data processed in the traditional (material) way and virtually by computers. Things that are obvious to those employees who are familiar with law and IT may not be obvious for other employees. Therefore, in addition to professional procedures of media storage, the documentation should include also the simplest tips, e.g. the need to delete data that are no longer needed, and the need for caution in the use of sheets of paper one side of which has already been printed.

The specificity of some workplaces also makes civil servants work outside the office in many cases. In such work, they also use documents containing personal data and other information that can be stolen and misused. That is why the Information Security Policy should include procedures referring to the situations in which employees will proceed with databases outside the office. When the list of data sets is properly made, Personal Data Administrators should also decide which files can be used out of the office and which of them require special permission to be used in such a way.

Nowadays, in local government, most office workers use a separate computer. A standard procedure includes creating a login and a password for every employee, called broadcasting of powers by the Administrator of Personal Data. In most cases, this procedure prevents from unauthorized access. Moreover, employees should follow

[18] Cf. J. Hollenbeck, B. Jamieson, 'Human Capital, Social Capital, and Social Network Analysis: Implications for Strategic Human Resource Management', *Academy of Management Perspectives*, vol. 29, no. 3, 2015, pp. 379-381.

two rules. The first is the regular change of a password which should be difficult to guess, e.g. the password may include many different signs (capital and small letters). The second rule is a clear indication that an employee can use only their ID even for close cooperation in the workgroup. Supervisors should not induce the feeling of fear in administrative officers.[19] They must, however, be fair and thoroughly acquainted with the consequences of improper dealing with databases. The consequences of violations of the ISP apply to all employees – for this reason InfoSec issues should be a priority.

2.4. IT system management instruction

The RMIA specifies the requirements for the two documents in each institution. The previously described Information Security Policy must be supplemented by the IT System Management Instruction. One question that arises, however, is whether all institutions need such an instruction, especially those in which the data are processed outside the computer system. The Regulation specifies precisely what information should be included in the instruction (it is listed in the points in section 2.3). The information does not raise doubts and provides instructions for employees on how to deal with the computer system to prevent unauthorized access and other threats in cyberspace. It is important and affects all aspects of InfoSec. The most important aim of preparing the document, however, is the adequate determination of a security level and relevant procedures. The Personal Data Administrator has a choice of three levels – basic, higher and the highest.

The basic level refers to institutions that in their computer systems do not process data which refer to the racial or ethnic origin, political opinions, religious or philosophical beliefs, a, party or trade union membership, or are related to health condition, the genetic code, addictions, sexual life, convictions, decisions on penalty and fines, related to other decisions issued in court or administrative proceedings. Moreover, in these institutions none of the computer system devices

[19] Cf. J. D'Arcy, H. Tejaswini, M. Shoss, 'Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective', *Journal of Management Information Systems*, vol. 31, no. 2, 2014, pp. 285-318.

used for processing personal data is connected to the public network, e.g. the Internet. If the basic level is appropriate to the institution, the Personal Data Administrator must establish the specific procedures. For example, the adequate protection of the area in which data are processed; the use of access control mechanisms; the assignment of IDs and passwords to the users; system protection against viruses; system protection against data loss; the change of passwords at least once every 30 days, the password consisting of at least 6 characters; data protection against copying; the adequate protection of backups and laptops; deleting data from devices to be thrown away.[20]

The higher level refers to institutions that in their computer systems process the data included in the basic level and none of the computer system devices used for processing personal data is connected to the public network, e.g. the Internet. If the higher level is appropriate to the institution, the Personal Data Administrator must establish the same procedures as in the basic level but with a few changes, e.g. a password consists of at least 8 characters, contains lowercase and uppercase letters, numbers and special characters.[21]

The highest level refers to institutions that in their computer systems process the data included in the higher level and only one of the devices is connected to the public network, e.g. the Internet. If the highest level is appropriate to the institution, the Personal Data Administrator must establish the same procedures as in the higher level and: 1) the computer system for processing personal data must be protected against threats coming from the public network by implementing physical or logical security features that protect it against unauthorized access; 2) the data controller shall implement measures for cryptographic protection to the data used for authentication that is transmitted over a public network.

Although the requirements are restrictive and there are a lot of problems in implementing them to some institutions of territorial self-government (described in detail in section 4.2), it is difficult to find another way to raise the level of InfoSec in them.

[20] Attachment no. 1 to the Regulation on Personal Data Processing Documentation, Technical and Organizational Conditions, which Should be Fulfilled by Devices and Computer Systems Used for Personal Data Processing of 29 April 2004, *Journal of Laws*, no. 100, 2004, item 1024.

[21] Ibid.

3. Implementation of the Information Security Policy in Polish territorial self-government

3.1. Different tiers of territorial self-government

The final point of this article consists of two parts. The first one examines the implementation of the ISP in different tiers of Polish territorial self-government. In the second part, the author presents the most important problems in the implementation resulting from financial reasons and the lack of qualifications of some civil servants.

The Republic of Poland is divided into 16 voivodeships (with 16 marshal offices), 379 counties, and 2479 communes. There are two kinds of counties, i.e. land counties (314) and cities with county rights (65). There are three kinds of communes, i.e. rural communes covering only rural areas, rural-urban communes which cover towns and rural areas, and urban communes covering only cities. Cities with county rights are also considered communes.[22]

Notably, Polish territorial self-government has a major role in implementing all legislative provisions connected with information security. This is due to the fact that most institutions are run by local government, not by the government, e.g. about 25 000 schools run by local government.[23] Moreover, the Office of the GIPDP is not able to check the adequacy of the documentation of most institutions related to the local government. The Office has an annual budget of 15 million PLN and employs only about 120 employees.[24] This causes a situation in which the local government has to introduce instruments and procedures, but also to control them. It is a huge responsibility for the InfoSec of many citizens.

The main idea of the ISP is to establish appropriate procedures in all the institutions, no matter if they are connected with territorial self-government, government or others. From this point of view, it does not matter whether this is the case of a commune, a county or a voivode-

[22] M. Wiśniewska, K. Szczepańska, 'Quality management frameworks implementation in Polish local governments', *Total Quality Management & Business Excellence*, vol. 25, no. 3/4, 2014, p. 356.

[23] The Author's calculations based on official data from the Ministry of Education in Poland (2012).

[24] Najwyższa Izba Kontroli [The Supreme Chamber of Control], 'Informacja o wynikach kontroli wykonania budżetu państwa w 2014 r. w części 10 – Generalny Inspektor Ochrony Danych Osobowych' [Information on the results of monitoring the implementation of national budget 2014 in section 10 – General Inspector for Personal Data Protection], Najwyższa Izba Kontroli (NIK), May 2015, p. 4, https://www.nik.gov.pl/plik/id,8931.pdf (2016-01-10).

ship, because the legal requirements are the same for the institutions of all the tiers of local government. Nonetheless, it is worth pointing out that there is a significant difference between the InfoSec issues in the voivodeship and the other two tiers of local government. As it is well known, there are two main types of institutions connected with voivodeships: voivodeship offices and marshal offices. The former is an office of the voivode and the local representative of the Prime Minister. The latter is an office of the province marshal and the province government chosen from the elections to the regional council. There are a number of important differences between voivodeship and marshal offices. The most important one is the theoretical possibility of the voivode to influence the law making. Even more important are the know-how, training programmes and courses from the government. From that point of view, regional offices are in an advantageous position. However, being separated from the government (marshal offices) also means having an independent view on InfoSec.

The analysis of the Public Information Bulletin of several voivodeship offices, incl. the Masovia Voivodeship, West Pomeranian Voivodeship, Lublin Voivodeship[25] and marshal offices, incl. the Marshall Office of the Greater Poland Voivodeship, the Marshall Office of the Little Poland Voivodeship, the Marshall Office of the Podlaskie Voivodeship[26] depicts that the ISP was implemented in the main offices and subordinated institutions. However, the effectiveness of the procedures can be only understood by testing the quality of information security incidents management. Indeed, important surveys were conduct-

[25] Lubelski Urząd Wojewódzki w Lublinie [Lublin Voivodeship Office], Biuletyn Informacji Publicznej Lubelskiego Urzędu Wojewódzkiego w Lublinie [Public Information Bulletin], http://luwwlublinie.bip.gov.pl/ (2016-10-23); Mazowiecki Urząd Wojewódzki w Warszawie [Masovia Voivodeship Office], Biuletyn Informacji Publicznej Mazowieckiego Urzędu Wojewódzkiego w Warszawie [Public Information Bulletin], http://bip.mazowieckie.pl (2016-10-23); Urząd Wojewódzki w Szczecinie [West Pomeranian Voivodeship Office in Szczecin], Biuletyn Informacji Publicznej Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecnie [Public Information Bulettin], http://szczecin.uw.gov.pl/bip (2016-10-23).

[26] Urząd Marszałkowski Województwa Wielkopolskiego w Poznaniu [The Marshall Office of the Greater Poland Voivodeship], Biuletyn Informacji Publicznej Urzędu Marszałkowskiego Województwa Wielkopolskiego w Poznaniu [Public Information Bulletin], http://bip.umww.pl (2016-10-23); Urząd Marszałkowski Województwa Małopolskiego [The Marshall Office of the Lesser Poland Voivodeship], Biuletyn Informacji Publicznej Województwa Małopolskiego [Public Information Bulletin], http://bip.malopolska.pl/umwm (2016-10-23).

ed[27] in marshal offices between December 2012 and April 2013 and in voivodeship offices between December 2013 and March 2014 to examine this issue.[28] The outcomes of the surveys suggest that only in 5 out of the 11 voivodeship offices, information security incidents had occurred and were registered. The authors of the survey[29] compared these data with the number of information security incidents confirmed by the Governmental Computer Incident Response Team reports. These were as follows: 2011 – 854 notifications, 249 incidents; 2012 – 1168 notifications, 457 incidents; 2013 – 8817 notifications, 5670 incidents.[30] It is alarming that in many voivodeship and marshal offices information security is treated as the priority. Indeed the authors of the survey concluded:

> "The offices, in which the information security incidents have not been registered, should implement an information security incident management as soon as possible because a lot of security incidents in public administration could happen"[31] and "Not all offices have the correct way of information security incidents management. In some units, this process is reduced only to notifying the relevant departments of the fact that the incident occurred. Some of the offices have implemented comprehensive incident management."[32]

The study of the implementation of laws related to InfoSec by the communes is difficult due to their large number. No government institution keeps statistics on this subject. As in the previous case, important information is provided by the Public Information Bulletin. After the analysis of selected communes' bulletins it can be concluded that in most cases there has been an implementation of the legal rules governing the matter of InfoSec. A number of communes treat

[27] Survey questionnaires were sent to all sixteen marshal offices and all sixteen voivodeship offices in Poland. 13 positive responses from marshal offices and 11 positive responses from voivodeship offices were obtained. Among the 13 marshal offices, only in 7 information security incidents had occurred and were registered.

[28] D. Lisiak-Felicka, M. Szmit, 'Information Security Incidents Management in Marshal Offices and Voivodeship Offices in Poland', *Studies & Proceedings*, Polish Association for Knowledge Management, no. 72, 2014, p. 28.

[29] Loc. cit.

[30] Ibid., p. 30.

[31] Ibid., p. 35.

[32] Ibid.

the issue of information security seriously, with a special focus on the protection of personal data. One example of this approach is the Lublin Commune. The President of Lublin carries out inspections of institutions subordinated to the Audit and Control Department of the City of Lublin. A detailed analysis of 52 protocols of the inspections carried out in 2013-2015 leads to a positive conclusion that in all cases the information security procedures were checked.[33] The inspectors' concerns referred to the lack of certain documents, usually annexes to the ISP. Although it is not a serious weakness, the awareness of being monitored encourages the heads of institutions to further work. It should be indicated as an appropriate action. However, there are many communes that do not pay much attention to the issue of InfoSec. Internal controls are used to verify only the financial statements and do not include even the most basic security issues such as the protection of personal data. In this case, the activity of communes can be verified in two ways in the future. The first one is the occurrence of incidents and crimes in cyberspace associated with local government and the procedures of practical verification. The second way is probably an increase in the GIPDP's budget by the government.

3.2. Implementation: selected problems and challenges

The implementation of the provisions on InfoSec with a special focus on the protection of personal data causes many difficulties. The catalogue of problems is wide and among the most important points the following ones should be mentioned: the financial aspects, incidents of heads' dishonesty and the lack of appropriate qualifications of civil servants. All these factors are strongly mutually related and very rarely occur as single ones. Since the political transformation, the phenomenon has been clearly seen of assigning tasks by the government to territorial self-governments without providing financial resources. Also, the restrictive provisions relating to information security have been introduced without proper preparation. The RMIA functioned only to a little extent in the early years of being in force. Many territo-

[33] Samorząd Miasta Lublin [Self-government of the city of Lublin], Biuletyn Informacji Publicznej Samorządu Miasta Lublina [Public Information Bulletin], http://bip.lublin.eu/bip/um/index.php?t=200&fid=13386 (2016-04-01).

rial self-governments were not prepared for the changes. The contract for the preparation of documentation by external companies was the only solution to the lack of experts in the institutions. Only the richest communes, counties and voivodeships have the financial resources to outsource such an action. It is a widely held view that the contract for the preparation of documentation by an external company involves total outsourcing. The main weakness of this theory is that companies dealing with data protection and the preparation of documentation need a lot of information about the institution. Preparing the Information Security Policy by an external company, therefore, requires a close cooperation and many of the tasks must be performed by the institution. However, most companies have to look for other solutions, which leads to an abusive and improper implementation of the procedures. Although more than 10 years have passed since the new laws entered into force, the problems still persist in many institutions. One of the most dangerous practices is copying the documentation from the Internet or other institutions. This is dishonest and damaging to the security of local government information. The aim of the article is not to evaluate the axiological dimension of this phenomenon. A serious weakness of copied documents, however, is that they are not adapted to the specificity of the institution. This contradicts the idea of the Information Security Policy as a guide for employees with the most important elements of InfoSec.

The final point concerns the problem of frequently inadequate qualifications of the civil servants. Over the past few decades, the quality of service in the territorial self-government administration sector has become an issue of great concern.[34] Citizens have a negative attitude towards civil servants, which is associated with their arrogant behaviour at the time of the Polish People's Republic. A factual overview of this issue requires an understanding of the other side. Many civil servants had worked in a different reality for many years. They have had to learn, for example, how to use computers in order to meet the increasing demands of citizens. Notwithstanding, their lack of qualifications has become one of the major difficulties in the implementation of the Information Security Policy in local government. The elimination of

[34] Wiśniewska and Szczepańska, op. cit., p. 352.

the main threats does not require specialized knowledge. It is often a matter of willingness and good will.[35] Among the most important problems were the unwillingness to learn new procedures explained by an excess of responsibilities, the violation of basic safety rules, e.g. directing the monitor towards customers even if it displays confidential information, the unwillingness to participate in trainings concerning InfoSec and citizens' reluctance to provide information. The situation will certainly improve in the future, as evidenced by the growing number of appointed Information Security Administrators and increased emphasis on upscaling the civil servant's skills.

Conclusions

The objective of this article was to examine the micro-dimension of InfoSec and to discuss the ISP as a necessary tool that complements it. The paper sought as well to determine the role of every single civil servant in InfoSec issues in Polish territorial self-government. It is worth remembering that scientific research cannot only focus on the IT aspects in the fight against cybercrime. There is still much work to do in local government institutions. It should be stressed that Polish institutions were given great tools. The establishment of information security laws, described in the article, shows that Poland has made great progress in this matter over the last decade. The APDP and the RMIA are modern and useful sources of law. The Information Security Policy in every institution enhances citizens' safety as far as the security of information is concerned.

Returning to the hypothesis posed at the beginning of this study, it is now possible to state that InfoSec of all citizens depends largely on the proper preparation and implementation of internal regulations of individual institutions. This idea has significant implications for the understanding of the actions which politicians and the heads of territorial self-government institutions should take to increase safety and security of the inhabitants of Poland. In this context, education of civil servants responsible for the security of information is worth pointing

[35] Cf. Y. Chen, K. Ramamuthy, K. Wen, 'Organizations' Information Security Policy Compliance: Stick or Carrot Approach?', *Journal of Management Information Systems*, vol. 29, no. 3, 2012, p. 159.

out, with special emphasis on the protection of personal data. What is more, HR processes should include elements aimed at qualified applicants for the protection of personal data. Considering the systematic increase in threats and cybercrime, internal documentation in institutions needs to be updated. These activities will help maintain a good rate of change and improve safety and security of citizens in the face of threats.

References

Chen, Y., Ramamuthy, K., Wen, K., 'Organizations' Information Security Policy Compliance: Stick or Carrot Approach?', *Journal of Management Information Systems*, vol. 29, no. 3, 2012, pp. 291-326.

D'Arcy, J., Tejaswini, H., Shoss, M., 'Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective', *Journal of Management Information Systems*, vol. 31, no. 2, 2014, pp. 291-325.

Fajgielski, P., *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony* [Information in public administration. Legal aspects of gathering, sharing and protection], Wrocław: PRESS-COM, 2007.

Hollenbeck, J., Jamieson, B., 'Human Capital, Social Capital, and Social Network Analysis: Implications for Strategic Human Resource Management', *Academy of Management Perspectives*, vol. 29, no. 3, 2015, pp. 370-385.

ISACA, *Glossary of Terms*, Information Systems Audit and Control Association (ISACA), http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (2016-01-04).

Kowalewski, M., Kowalewski, J., *Polityka bezpieczeństwa informacji w praktyce* [Information security policy in practice], Wrocław: Aspra-Jr, 2014.

Leshem, N., Pinkreteon, A., 'Re-inhabiting no-man's land: genealogies, political life and critical agendas', *Transactions of the Institute of British Geographers*, vol. 41, no. 1, 2016, pp. 41-53.

Lisiak-Felicka, D., Szmit, M., 'Information Security Incidents Management in Marshal Offices and Voivodeship Offices in Poland', *Studies & Proceedings*, Polish Association for Knowledge Management, no. 72, 2014.

Millard, F., 'Presidents and Democratization in Poland: The Roles of Lech Walesa and Aleksander Kwasniewski in Building a New Polity', *Journal of Communist Studies & Transition Politics*, vol. 16, no. 3, 2000, pp. 39-62.

Pawlak, P., 'Governance of Safety and Security in Cyberspace', in: P. Dąbrowska-Kłosińska (ed.), *Global safety governance: Challenges and Solutions*, Centre for Europe, University of Warsaw, Warszawa: Aspra-Jr, 2015.

Regulska, J., 'Governance or Self-governance in Poland? Benefits and Threats 20 Years Later', *International Journal of Politics, Culture & Society*, vol. 22, no. 4, 2012, pp. 537-556.

The Act on Personal Data Protection of 29 August 1997, *Journal of Laws*, 2014.

The Constitution of the Republic of Poland of 2 April 1997, *Journal of Laws*, no. 78, 1997.

The Regulation on Personal Data Processing Documentation, Technical and Organizational Conditions which should be Fulfilled by Devices and Computer Systems Used for Personal Data Processing of 29 April 2004, *Journal of Laws*, no. 100, 2004.

Najwyższa Izba Kontroli [The Supreme Chamber of Control], 'Informacja o wynikach kontroli wykonania budżetu państwa w 2014 r. w części 10 – Generalny Inspektor Ochrony Danych Osobowych' [Information on the results of monitoring the implementation of national budget 2014 in section 10 – General Inspector for Personal Data Protection], Najwyższa Izba Kontroli (NIK), May 2015, p. 4, https://www.nik.gov.pl/plik/id,8931.pdf (2016-01-10).

Wiśniewska, M., Szczepańska, K., 'Quality management frameworks implementation in Polish local governments', *Total Quality Management & Business Excellence*, vol. 25, no. 3/4, 2014, pp. 354-365.