sciendo

Personal data protection as an element of management security of information

doi:10.2478/mape-2019-0052
Date of submission to the Editor: 04/2018
Date of acceptance by the Editor: 07/2018
MAPE 2019, volume 2, issue 1, pp. 515-522

Justyna Żywiołek*
ORCID ID: 0000-0003-0407-0826
Czestochowa University of Technology, Poland

INTRODUCTION

Providing information has always been one of the key conditions for proper management of both the state and each organization. At a time when the main source of information was a pictogram, it was generally available, later the information was limited to a letter sent by the messenger. Over time, much faster and safer data transfer methods were developed, but this factor has always been the weakest link in the entire system. Currently, the development of teleinformation systems allows to eliminate errors to a large extent. However, it should be emphasized that people are still recipients and creators of information. At present, two basic areas of data loss can be distinguished.

The first is a deliberate attack on the information storage system by attacking data centers, the second is a targeted attack on the labor force using the fishing method for this purpose. The development of ICT has given man a range of possibilities for purposeful action. Information stored in information systems is among the most vulnerable to various types of attacks. That is why it is so important to secure information in every company. The most common methods currently used by criminals are: computer fraud, destruction of data or computer programs, computer sabotage, burglary into the computer system, eavesdropping.

INFORMATION SECURITY MANAGEMENT

Safety in the ordinary sense is understood as a state of non-threat and has been desired in many spheres of human activity for centuries (Żywiołek, 2017). In the context of information security, we talk about about the efficient functioning of processes in the organization. In the literature, information security is defined as "the quality of an organization free from threats related to information security" (Mottord, Whitman 2008). An important element of information protection is also its purpose, that is, protection of valuable information for the organization – information, but also the environment created by hardware and software (Humphreys,2007).

While defining the information security, a number of aspects were indicated, above all confidentiality, authenticity, availability, integrity, responsibility, reliability (Żywiołek, 2019). Whitman and Mottord (2008) also point to privacy as one of the aspects that need protection because of the relationship with the person. Personal information is

* j.zywiolek@gmail.com

information resources that have their own sensitivity, which is defined as a measure of importance assigned to information by its author or trustee in order to indicate the need to protect it (Białas, 2007).

SECURITY OF PERSONAL DATA

Meeting the legal requirements is the responsibility of every entrepreneur. With regard to systemic information security management, this is a key aspect that should be considered when choosing the security (included in the declaration of use), risk assessment, etc (Zou P., Lun P., Cipolla D., Mohamed S., 2017). Many legal acts concern a larger or smaller group of organizations, for example in the field of protection of classified information, intellectual property or the sphere of e-commerce and services, as well as specific areas of activity – e.g. banking and insurance services. Almost all organizations process personal data, therefore they must meet the relevant requirements set at the level of the law and regulations.

The current Act on the protection of personal data comes from May 2018. Originally, it was the implementation of the RODO Regulation, which obliged Poland to indicate how to achieve its objectives.

From May 2018 many companies have noticed that they are processing personal data. During the implementation of the RODO, many trainings were carried out, data protection inspectors were massively appointed, creating information security systems. However, employee awareness still indicates that the awareness should be built.

AWARENESS ABOUT PROTECTION REQUIREMENTS PERSONAL DATA

From May 2018, the author conducted research on information security management and employee awareness in this area. Research focused on the approach of small and medium enterprises to solutions in the area of information security. One of the aspects examined in the study is the assessment of awareness, motivation and solutions in the field of personal data protection.

110 production, service and trade enterprises from various industries were subjected to research. The study was conducted using an online survey.

The thesis adopted in the study refers to the level of employee awareness in the field of information security.

41 small enterprises, 44 medium-sized enterprises and 25 micro-enterprises participated in the survey. In the tested sample, 11 had a certified quality management system (eg ISO 9001 or ISO 20000-1), 5 of which were certified for compliance with ISO 14001, and two have an information security management system in accordance with ISO/IEC 27001.

Answers to the question about the processing of personal data are terrifying. As many as 24 companies denied data processing, 44 said they did not know, and even half of the respondents did not confirm processing. Worrying is the fact that 61 respondents confirmed that they process employee databases, 74 clients and 28 for product users. It should also be noted that respondents do not correctly use definitions relating to basic issues, in particular as regards the processing of personal data, e.g. they do not recognize that archiving is also an element of data processing. Moreover, in many cases the respondents were not able to separate the situation when the organization they represent is the data controller and processes the data based on entrustment. In

most cases, respondents who process data do not have written authorization. In 35 cases, respondents indicated that leadership plays a key role.

PERSONAL DATA PROTECTION AS PART OF AN INTEGRATED QUALITY AND INFORMATION SECURITY MANAGEMENT SYSTEM

Monitoring the security status requires the identification and identification of information security elements. Important elements of the information security management process are resources, threats, vulnerabilities, consequences, risks, safeguards and residual risk. There are many factors affecting the level of employees' awareness in the field of security. Based on the observations made in the surveyed enterprises, a relationship diagram was developed, including factors affecting the awareness of employees of the surveyed enterprises in the area of information security (Figure 1).

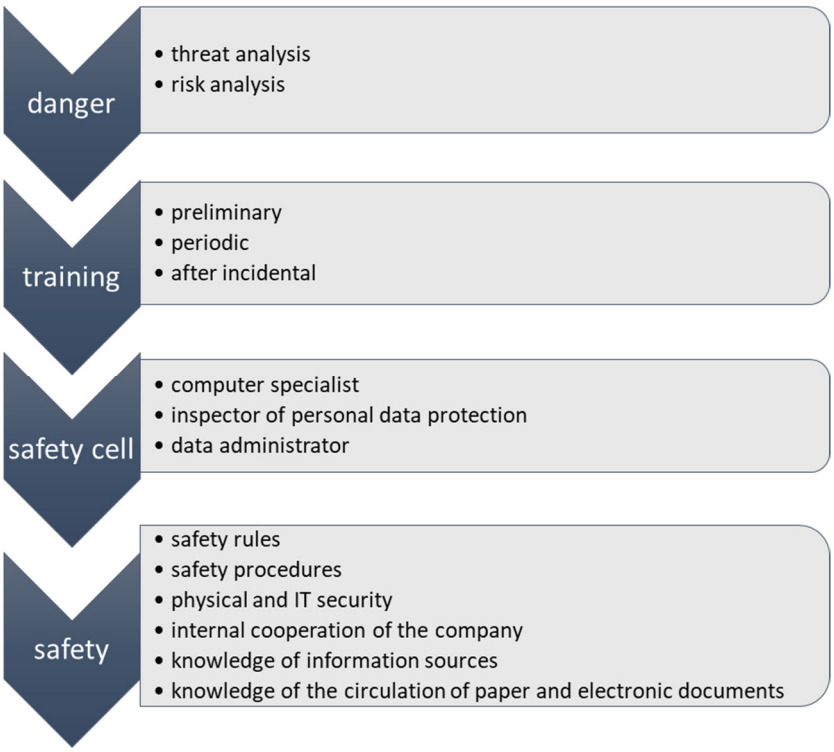

Fig. 1 Relationship diagram for information security

Based on the observations carried out in the surveyed enterprises, factors influencing information security were identified. These elements have been divided into four groups: security, security cell, training and threats. Based on them, factors influencing employee awareness in the field of information security were defined (Jędrzyjczyk, Kucęba, 2016).

In order to properly manage information in the company, which is the basis for ensuring information security, it seems advisable to examine satisfaction with information management among employees. Respondents gave the following answers to this question (Figure 2).

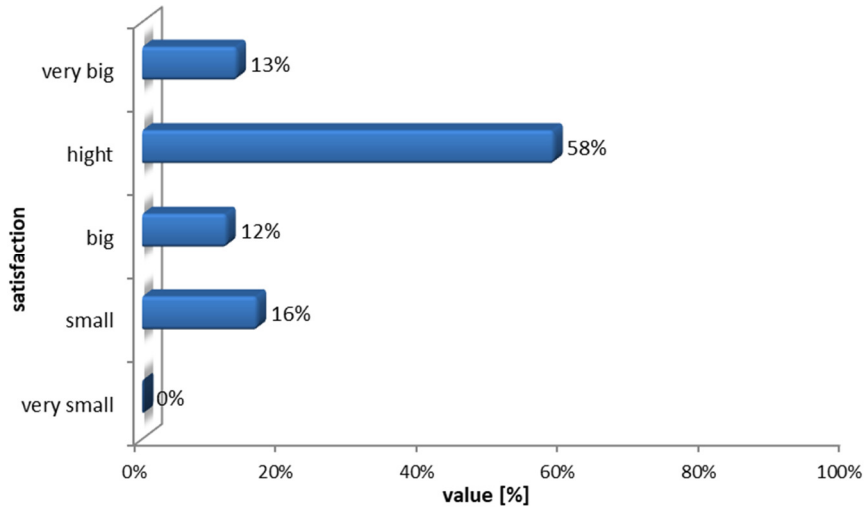

Fig. 2 Employee satisfaction with information security measures in the surveyed enterprises

The survey showed that employees understand the importance of information management for the proper functioning of the enterprise. Only 16% of employees of the surveyed enterprises do not see the importance of information security for enterprises.

Twenty-four respondents point to the appointment of an inspector of personal data protection, and in those cases the duties and authorizations that contained legal requirements were precisely defined. It is therefore necessary to provide the inspector with adequate permissions.

Forty-two respondents confirmed that they clearly defined the roles, responsibilities and authority to ensure information security. However, in 64 cases, respondents indicated that management plays a key role. Over 25% of respondents did not specify liability in this respect. The results are not unambiguous, and a certain hint in the interpretation of the results is the extremely low level of awareness regarding the requirements for the security of personal data.

Quoting the results of the research, it should be noted that according to the declaration almost half of respondents submit data outside Poland, including 37 to the EU and 14 to third countries. With such a low awareness of respondents in terms of requirements, one can draw a conclusion about very likely discrepancies in this respect.

The answers given to the question about having the necessary documentation can be clearly evaluated. Only 8 respondents declared having the required personal data security policy, but not all of them already have instructions for managing the IT system. 21 respondents stated that the requirement did not apply to them, and 15 - that they did not establish the mentioned documents. The analysis of this type of documents is even more striking. Most often, this is only a formal fulfillment of requirements, which is prepared in accordance with the formula, which has not been even the least adapted to the realities of the organization. Most often it is a manifestation of complete ignorance.

In individual cases, this fact results from the regulation of the principles of supervision over personal data in the documentation of the information security management system.

PROTECTION OF PERSONAL DATA AS AN INTEGRATED ELEMENT QUALITY MANAGEMENT SYSTEM AND INFORMATION SECURITY

The company is a recognized and large supplier of many types of steel. It has branches all over the world. One of the key branches is located in Poland, and is primarily responsible for sales and customer service in Europe.

The specificity of the organization is best reflected in its process map developed as part of the quality management system and information security management, as well as objectives related to standardization and performance measurement.

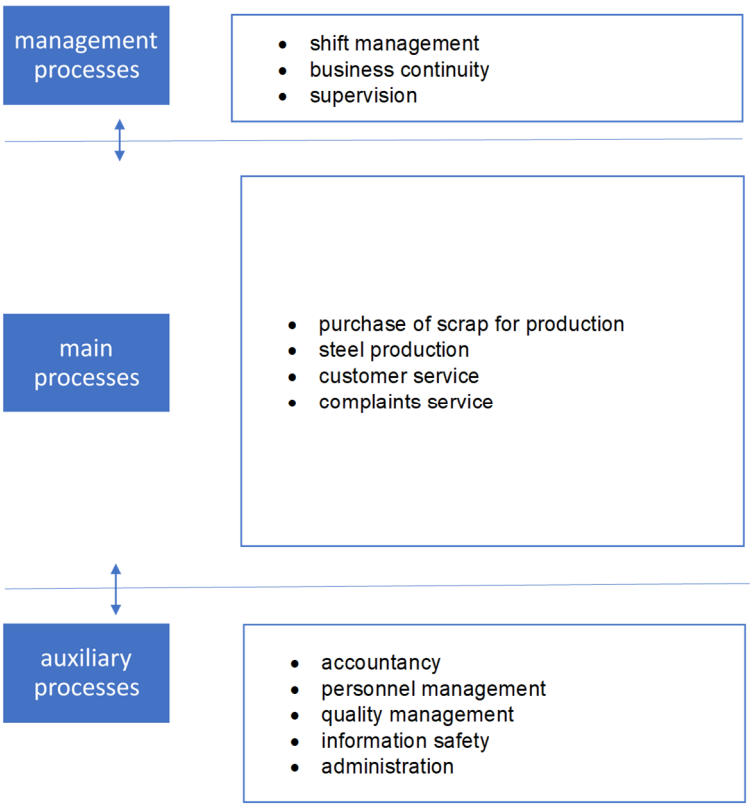

Fig. 3 The map of the processes of the examined enterprise

The key processes are technological solutions, which in effect are related to the production and processes of steel processing. It is a group of processes: production, machining ensuring its quality, sales.

The main processes are built by processes: qualitative research, technical support and customer service.

In addition, a process of superior nature has been defined - change management, which combines the need to respect the guidelines applicable in the entire corporation and management within the organization in Poland.

QUALITY MANAGEMENT, INFORMATION SECURITY AND PROTECTION OF PERSONAL DATA

The company clearly divided roles in the field of quality management, security and statutory liability related to the protection of personal data. The key role in this respect is played by the Quality and Information Security Manager, who is also the inspector of personal data protection. In practice, therefore, this person is solely responsible to

the management for the implementation, maintenance and development of the management system and has taken over the vast majority of the organization's responsibilities (operator of personal data).

As part of the management system, there are also (Gryszczyńska, Szpor, 2017):

process owners – responsible for the management of a given process, ranging from documentation and ending with measurements;

owners of databases of personal data – designated employees responsible for databases containing personal data. They are also responsible for reporting persons who must be authorized to process data;

members of the security forum – are responsible for assessing information security threats, agreeing and accepting risk management plans. The security forum also prepares a management review that takes place step by step during the weekly board meetings.

In practice, Quality and Information Security Manager is the coordinator of highly dispersed activities located within individual processes. According to the adopted assumptions, the tasks implemented by him were included in the group of ten priority tasks for the development of the organization (Pawełoszek, 2014):

- process approach and documentation of the ISMS - assumes verification of the process map and subordination to its assumptions of optimization and effectiveness measurement due to the fact that the former was subordinated only to the requirements of the standards constituting the basis of the system;
- risk management – risk management plans based on the results of risk assessment are not a real, readable element of system improvement;
- personal data management – thanks to the awareness of the amount of data processed as the operator of personal data and entrusted by the headquarters of the organization and due to the universal transfer of data outside the EU zone.

The requirements for the protection of personal data are fully integrated with the quality management system and information security, which guarantees the responsibility of one person directly before the management. The key documents related to the supervision of personal data are the personal data protection policy and IT network supervision instructions - developed as part of the quality management and information security process, it is important to recall many documents in them.

In the discussed company, the documentation model is described on two levels. The first level is the features of processes in the form of so-called Process manuals that refer to policies and instructions. The key documents regarding the protection of personal data are primarily recalled (Kępa, 2015):

- declaration of the application, which defines all the safeguards applied in the organization, including security regarding IT networks and, more broadly, ICT;
- business continuity and DRP (disaster recovery plan) plans;
- instructions for dealing with information security incidents;
- a catalogue of services including minimum parameters of service provision, including SLA (standard level agreement);
- instructions for monitoring and assessing the effectiveness of IT security.

According to the requirements, ABI is responsible for maintaining databases, including personal data. They are specified in the supervised file as so-called Open register. Each database is characterized by the name, main user, list of persons

authorized to process personal data, indication of the database administrator, identification of the purpose of data processing, population characteristics, contained database, the type of data collected in the database and data structure. In addition, a number of other more detailed features complement the register. It is extremely difficult to ensure effective supervision over it, it is a serious problem, as it concerns almost 50 databases and almost 250 employees, co-workers, often outside the company or the EU zone.

CONCLUSION

Information security is an important aspect of business management. Considering its specificity, it may be critical due to the market value which may affect the competitive advantage. Personal data must be protected in any case, for example due to the requirements set out in legal aspects. The answer to market needs and even requirements are systemic solutions in the field of data security management. They can be based on the internationally recognized ISO/IEC 27001 standard. Several groups of requirements must be met when implementing, maintaining and developing an information security management system. A prerequisite for the establishment and implementation of an effective information security management system is the fulfillment of legal requirements, including those relating to the protection of personal data. The results of research conducted by the author on a sample of selected enterprises with an additional analysis of one of them indicate a very low awareness of employees regarding the need to protect personal data, which may result in insufficient care for the rights of their owners. Recklessness in this area is manifest even in ignorance of the legal basis, establishing and documenting the required policy and instructions, and maintaining database records. Critical incompatibilities occur in the examined enterprises; in this case, representatives of the operator of personal data may be subject to criminal liability and loss of market credibility.

REFEENCES

Białas, A. (2007). Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie,

Gryszczyńska, A. and Szpor G. (2017). Internet. Strategie bezpieczeństwa. Warszawa: Beck.

Humphreys, E., Implementing the ISO/IEC 27001Information Security Management System Standard, Artech House, Norwood.

ISO/IEC 27001 (2013). Information technology – Security techniques – Information security management systems – Requirements.

Jędrzyjczyk, W. and Kucęba R. (2016). Teaching Managerial Competences at Universities, Trends of Management in the Contemporary Society.

Kępa, L. 2015. Ochrona danych osobowych w praktyce. Warszawa: Difin.

Mottord, H.J. and Whitman, M.E. (2008). Management of Information Security, 2nd ed., Boston: Thomson.

Pawełoszek, I. (2014). Semantic Organization of Information Resources for Supporting the Work of Academic Staff, Annals of Computer Science and Information Systems. Warszawa: WNT.

Wołowski, F. and Zawiła-Niedźwiecki J. (2015). Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi. Warszawa: edu-Libri, pp. 45.

Zou, P., Lun, P., Cipolla, D. and Mohamed S. (2017). Cloud-based safety information and communication system in infrastructure construction, Safety Science, 98.

Żywiołek, J. (2016). Międzyorganizacyjna wymiana informacji jako element zagrożenia bezpieczeństwa informacji [in:] Systemy bezpieczeństwa w podmiotach gospodarczych. Częstochowa: Oficyna Wydawnicza Stowarzyszenia Menedżerów Jakości i Produkcji, pp. 78.

Żywiołek, J. (2017). Zarządzanie wiedzą o systemie bezpieczeństwa i higieny pracy w przedsiębiorstwie. In: Światowy Dzień Bezpieczeństwa i Ochrony Zdrowia w Pracy, pp. 114.

Żywiołek, J. (2019). Monitoring of Information Security System Elements in the Metallurgical Enterprises, MATEC Web of Conferences. Available at: https://www.matec-conferences.org/articles/matecconf/pdf/2018/42/matecconf_qpi2018_01007.pdf.

Abstract. The article highlights the importance of information and the need to manage its security. The importance of information requires a systemic approach, which is why the standards of conduct for managing information security have been approximated. The results of research on information security management in the field of personal data protection have been presented. The research was carried out on a sample of 110 enterprises. The survey was extended to include an analysis of one of the companies subject to the survey. In the following, the case study regarding the production enterprise was also presented.

Keywords: security of information, personal data, security management