DE GRUYTER
OPEN

MANAGEMENT SCIENCES NAUKI O ZARZĄDZANIU

Year 2018, Vol. 23, No. 1
ISSN 2080-6000
e-ISSN 2449-9803

MANAGEMENT OF SECURITY OF THE BUSINESS INFORMATION AS EXEMPLIFIED BY THE NATIONAL DEBT REGISTER OF THE BUSINESS INFORMATION BUREAU JSC

Katarzyna Jasińska

Wrocław University of Economics, Wrocław, Poland
e-mail: katarzyna.jasinska@ue.wroc.pl

Martin Kaczmarski

University School of Physical Education in Wrocław, Wrocław, Poland
e-mail: martin@kaczmarski.pl

DOI: 10.15611/ms.2018.1.04
JEL Classification: K22, M15

Abstract: The aim of the article is to characterize the specificity of business information and issues related to ensuring their security on the example of the Business Information Bureau. The analysis covered the National Debt Register of Business Information Bureau S.A., which is the first and one of the largest entities of this type operating in Poland. The article first discusses the specific nature of business information as a special type of information regulated by the Act dedicated to it. The following part analyses the functioning of information security systems and procedures in the company's business information security. This analysis is to illustrate how the requirements imposed on business information offices were implemented in practice in the scope of an information security management system.

Keywords: business information, economy, Bureau, information, business, security, information security.

1. Introduction

Information is of vital importance for modern enterprises competing in the realities of a knowledge-based economy. The ability to acquire, process and apply it can determine the position of an entity in a market or individual in a society defined as the Information Society.

The success of each entity's activity depends, to a large extent, on finding sources of reliable information, early acquisition, selection and proper flow and the use of it [Szustak 2014].

Information has become one of the most valued assets in business, and issues related to the management of its security have been at the centre of interest of both management, IT and legal research as well as practical solutions in enterprises [Oleński 2001; Bekas 2011; Szustak 2014; Kowalewski, Ołtarzewska 2007; Humphreys 2008; Bertino 1998; Velumadhava Raoa, Selvamanib 2015].

This trend fits in with the aim of the article, which is to characterize the specificity of business information and issues of ensuring their security.

In the article, as a research method, the analysis of the Business Information Bureau, the National Debt Register of Business Information Bureau JSC, in which the security of information processing plays a key role, was selected. The vast amount of data, very sensitive and economically important, processed in this type of entity requires the most advanced solutions. Additional requirements for information security offices are connected with the implementation

of Regulation (EU) 2016/679 of the European Parliament, and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (the so-called GDPR). The new regulation will apply from 25 May 2018, so the data security systems in enterprises need to be adapted accordingly. The topic discussed in the article is therefore a relevant one from the practical point of view, although the aim of this paper is not a detailed analysis of the requirements in relation to the implementation of GDPR.

On the basis of literature analysis, the article discusses the specificity of business information as a particular type of information and analyses the functioning of information protection systems and procedures in the Business Information Bureau. Legal requirements and principles of logical, physical and procedural protection are presented, which allow to ensure the proper security of business information in the company. Theoretical deliberations have been supplemented by a discussion of the solutions implemented in practice in the National Debt Register of Business Information Bureau JSC.

2. The concept and characteristics of business information

The notion of information is an ambiguous term. It works in everyday language and in many different branches of science. Referring to the definition of classical information, this information is analyzed and processed into a form understandable to the recipient, which notifies him/her about the situation and has a value in the decision-making process, contains facts and figures which are presented in a form which is understandable to the recipient, concerns his/her area of interest and has a value for him/her and at the same time does not duplicate his/her knowledge resources [Sopińska 2004].

Business information is a specific type of information. Referring to the sources of law, pursuant to Article 2 of the Act of 9 April 2010 on facilitating the business information and exchanging economic data (consolidated text: Journal of Laws of 2014, item 1015 as amended, further as A.f.b.i.), "business information" refers to, among others, an entity which is a legal person or an organizational unit without a legal personality. These include the company name, address, selected personal data of partners, company registration details and a description of the object of its activities[1].

Business information is not only an indication of the current condition of a given entity by indicating its selected parameters. Apart from the current dimension, it also has a retrospective and prospective dimensions.

In the context of the past, business information refers to financial liabilities. It provides data on the amount and date of arrears, information on the disposal of receivables and other information on the proceedings concerning liabilities, and their questioning[2]. It also describes information on events such as using a counterfeit or third party's document[3] [i.e. f.]. In a prospective dimension, business information provides knowledge about the payment reliability of the counterparty, which in turn may have an impact on "the future of the entity in the context of its development or its investment and creditworthiness (cf. [Białek, Marzec 2011, p. 22]).

From a management perspective, business information is a specific type of information which can be understood as any information about systems, processes and events occurring in the economy; any information used by economic decision-makers; any information used to control economic processes or systems; orchestrating information in economic

[1] Pursuant to the Act, business information is the name or company name, registered office and address, number of the relevant register, tax identification number, names, surnames and PESEL insurance identification numbers of the partners, members of the management board or proxy, names and surnames of appointed proxies, main object of business activity. In the case of natural persons, economic information includes data on names and surnames, address of residence or delivery, PESEL insurance number or other identification number, series and ID number. Business information about natural persons conducting business activity is the name, surname, PESEL number, series and number of the identity card, the company, the name of the place of residence, address for delivery or the address for performance of business activity, tax identification number, REGON number, number of the relevant register, names and surnames of the attorneys, if they have been established, the main object of business activity.

[2] Pursuant to Article 2 of the Act, this includes in particular information on legal title, amount and currency, amount of arrears, date of arrears, information on proceedings concerning liabilities, information on questioning the existence of the whole or part of the liability, date of sending a payment request with a warning about the intention to pass the information to the Business Information Bureau, information about the sale of receivables, as well as other information.

[3] Pursuant to Article 2 of the Act, it includes the name of the document, its series and number, the date of issue, its registered office and address of the entity indicated in the document as an issuer, names and surnames of the person which the document concerns, the circumstances of using the document, indication of a person or body stating that the document has been falsified, or the fact that it belongs to a third party.

systems necessary for their existence and functioning; and information causing economic effects [Oleński 2001]. The literature indicates that "The primary role of business information is to provide knowledge about the payment reliability of the counterparty" [Białek, Marzec 2011, p. 22].

To sum up, the set of data constituting business information is characterised by a wide variety and scope. This collection, which includes a wide range of different data and, at the same time, important personal data, which are subject to strict protection under different legal regulations.

Incorrect processing or use of business information may pose a high risk to the company, e.g. by damaging reputation or by extortion. Therefore in companies processing business information, the information management system must meet a number of specific legal and organizational requirements.

3. Business Information Bureaus. Genesis and legal basis of functioning

In connection with numerous problems which arose in the area of financial flows in Poland after 1989, regulations were introduced which made it possible to set up Business Information Bureaus, whose task is to mediate in the provision of business information, consisting in receiving such information from creditors, storing and disclosing information. The main reasons for the establishment of these entities were growing problems of insolvency of business entities, increasing number of bankruptcies, blacklist of debtors on the internet, as well as the background of developed capitalist countries [Bekas 2011].

The passing of the Act of 14 February 2003 on business information disclosure (Journal of Laws No. 50, item 424 as amended) made it possible to establish the National Debt Register of Business Information Bureau JSC, which commenced its activity on 4 August 2003. In the following years further BIB entities were established: InfoMonitor JSC of Business Information Bureau, National Business Information Bureau JSC, ERIF Debt Register of Business Information Bureau JSC, and also National Telecommunication Debt Information of Business Information Bureau JSC.

Among the competences of the Business Information Bureaus, there is first and foremost:

- intermediation in making business information available, consisting of receiving business information from creditors, storing and disclosing this information (Article 7 of the Act),
- processing of archival business information for statistical purposes, managing the assets of the office,
- conducting training or educational activities, including the scope of the Bureau's activities.

Pursuant to Article 4 of the Act, it is possible to make business information available to third parties only through BIB, unless this is done in order to sell the debt claims by way of a public announcement or unless the regulations provide for a different procedure. Article 12 of the Act, on the other hand, states that the possibility of accepting the data on debtors from creditors is only possible if the relevant agreement is concluded in writing.

Legal sources specify in detail what requirements must be met in order for business information to be collected, processed, disclosed and subsequently deleted. In particular, these requirements specify:

- Conditions to be fulfilled by the counterparty when accepting an application in the register of debtors, which depend on the legal status of the resulting obligation and the status of the counterparty (Articles 14 and 15).
- Guidelines for ensuring appropriate communication with the debtor, in particular the form, time and scope of correspondence and contact (Article 16).
- Method and conditions of disclosure (Articles 21 and 22).
- Form and scope of the information to be extracted and transmitted, relating to access to the PESEL database and recordkeeping of a queries register (Articles 27 and 28).
- Removal of information and indication of the conditions under which data must be erased (Article 31).

A proper interpretation of the regulations concerning the above mentioned requirements imposed on Business Information Bureaus is subject to legal discipline. From the point of view of management discipline, it is of the essence that these requirements influence the way the information security management system functions, which needs to be adapted accordingly. The implementation of data security solutions in practice is subject to considerable amenability, including criminal amenability in the case of infringement. The requirements for information processing systems in Business Information Bureaux will be discussed in another part of the article.

4. Security of business information processing in Business Information Bureaux

Information security can be defined as preserving confidentiality, integrity and availability. Information confidentiality is about providing access to information only to authorised persons and accessibility means that

the authorised persons have access to information only when necessary. Integrity is a guarantee of accuracy and completeness of the information itself and its processing methods [Kowalewski, Ołtarzewska 2007]. The ISO/IEC 27001:2005 standard which was issued by the International Organization for Standardization and International Electrotechnical Commission in 2005 is the international standard in the management of information security. This standard provides guidance for the development, implementation, management, monitoring and review of an organisation's information security management system, regardless of the sector in which it operates. The guidelines of the standard must be implemented under the actual conditions of each undertaking.

In the case of entities such as Business Information Bureaux, ensuring data security concerns all elements of the company's information management system, since this type of company is based on the data processing process in its core business. Data is collected from the environment, then processed and made available outside the enterprise. Within each of these stages, products and services are created to be offered to customers, their sales allow them to generate profit. Disturbance of any legal process may involve criminal amenability, while in the market dimension it may involve loss of position and loss of customers. According to the ISO/IEC 17799 standard, an enterprise information management system is part of an overall management system developed on a business risk approach relating to the establishment, implementation, operation, monitoring, maintenance and improvement of information security [PN-ISO/IEC 1779:2007]. Maintaining information security in a business information bureau should be considered at the enterprise level. In addition to the basic security requirements of integrity, confidentiality, data availability and incident prevention, it is required to ensure viability and freedom to pursue the enterprise's own objectives, in particular by exploiting opportunities, reducing risk and preventing any kind of threats to the subject and its data processing interests (see [Koziej 2011]).

In general, three main areas can be identified within the information protection system: human, process and technology areas [Nowak, Scheffs 2010]. Security is related to all areas of the entity's activity, therefore the structure of the information security system must be based on the characteristics of the company [Koziej 2011]. In the case of business information bureaux, this system is significantly affected by legal obligations and obligations stemming from the need to ensure the physical, logical and technical protection of information processing.

Management of the information security system in the Business Information Bureau, the generalized

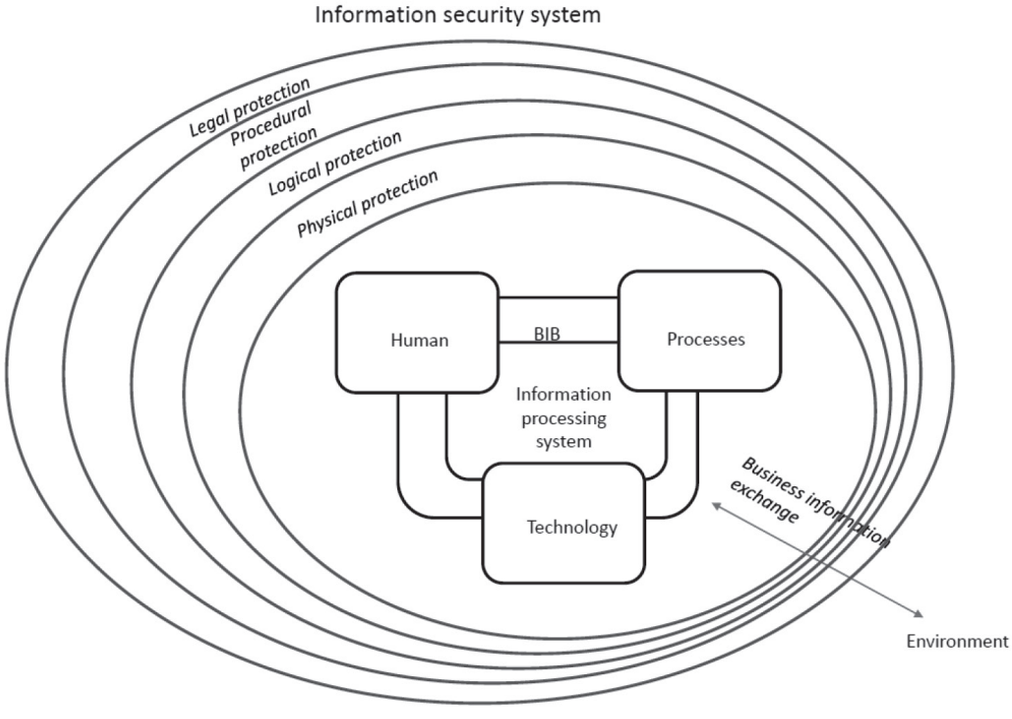

Fig. 1. Generalized model of information security system in BIB

Source: own work based on [Nowak, Scheffs 2010].

model of which is presented on Figure 1, takes into account the following types of protection of business information[4]:

- Legal protection, related to the compliance with the requirements of the law, appropriate to the characteristics of the data processed.
- Physical protection by restricting access to data processing equipment by protecting the information processing system against random events such as fires, floods or other threats.
- Logical protection, which aims to create various types of user authorisation mechanisms aimed at restricting access to data only to authorised persons.
- Procedural protection, which serves to sanction the rules on physical and logical protection. It introduces a basic classification of data, i.e. a process that allows for the precise determination of the level of saliency of data for an organization in order to be able to apply appropriate protection mechanisms for them.

The model shown in Figure 1 is a complex but not redundant scheme. Its logic is in line with the assumptions of the ISO/IEC 27001:2005 standard. The layers proposed in the model are to serve as a reference to the characteristics of specific conditions faced by information security offices in data security management, they refer to all elements presented in Figure 1 – people, technology and processes. Business Information Bureaux have to meet the list of requirements within each layer of the model.

It should be stressed that the most sensitive element of the presented model is human. Much has been written regarding human influence on even the most complex information security systems in the source literature [Colwill 2009; Liginlala, Simb, Khansac 2009].

The individual layers of the model will be discussed further on the example of the National Debt Register. This will allow to identify detailed solutions implemented within each of the discussed areas.

5. Security of business information in practice; the example of NDR BIB JSC

The analysis covered the National Debt Register of Business Information Bureau JSC, which was the first entity on the Polish market to perform the tasks of a business information bureau. The entity processes information that is protected by various legal acts, not only concerning business information but also the protection of personal data and classified information. The company competes on the market by building a wide range of services related to the provision of information, which are dedicated to different groups of customers. The company is a part of the Kaczmarski Group, whose individual entities offer services of collection, factoring and sharing of various types of information in traditional and electronic channels (see: [https://krd.pl/, date of access: 10.12.17]).

Implemented in NDR BIB JSC, the information security management system meets a number of legal requirements and ensures physical, logical and procedural data protection. The National Debt Register is certified in accordance with the ISO/IEC 27001:2005 standard. The selected elements of the system and the solutions implemented within it will be discussed further.

5.1. Legal obligations

Information security may be defined as preserving the confidentiality, integrity and availability of information, provided that confidentiality means ensuring that only authorised persons have access to the information, while the availability of information means that authorised persons have access to the information only when necessary. Integrity is understood as ensuring the accuracy and completeness of the information itself and its processing methods [Kowalewski, Ołtarzewska 2007].

Pursuant to Article 11 of the Act on business information disclosure, the Board of Directors of BIB is obliged to adopt data management regulations, which shall specify, among others, the ways of securing business information. These regulations must be approved by the decision of the minister in charge of economy, after consultation with the Minister of Justice and the Inspector General for Personal Data Protection. In the event that the regulations are inconsistent with the Act or separate regulations, the minister in charge of economy may refuse to approve the act.

NDR's data management regulations are available on the company's website, giving potential customers the opportunity to gain knowledge of flow procedures and the rules of information sharing. Moreover, these regulations are not the only document, since in accordance with paragraph 26 thereof, in order to properly manage information security, the NDR has

[4] The layers proposed in the Layer Model refer to areas of particular importance for information security management in Business Information Bureaux. Reference to normative assumptions alone would not reveal the complexity of requirements which Business Information Bureaux are facing when implementing information security management systems.

developed and implemented numerous documents which define the principles of security in the processing of information. In accordance with paragraph 27 of the regulations, the NRD has developed and implemented the IT System Management Instruction, which defines the procedures for granting rights to process the acquired data, as well as recording these rights, together with the identification of persons who are responsible for these activities; the methods and authentication measures applied in the company together with management and usage procedures; the procedures for starting, suspending and terminating the work for the system users or the procedure of creating back-up copies of data sets and NDR systems.

Moreover, one of the most important legal acts related to information security issues is the Personal Data Protection Act of 29 August 1997 (consolidated text: Journal of Laws of 2016, item 922 with subsequent amendments, further P.D.P.A.). Pursuant to Article 3 of P.D.P.A. in matters not regulated by this Act, the provisions on personal data protection shall apply. This Act is also referred to in Chapter VII of the Data Management Regulations of the NDR; paragraph 21 states that in matters not regulated with regard to the processing of personal data, Articles 36 to 39 of the Act shall apply in particular.

Art. 36 of P.D.P.A., states that "The data administrator shall be obliged to apply technical and organizational measures ensuring the protection of personal data processed, appropriate to the risks and categories of data covered by the protection, and in particular shall protect the data against their disclosure to unauthorized persons, obtaining by an unauthorised person, processing with the violation of the Act and the change, loss, damage or destruction". As noted in the literature, the legislator has left a certain freedom of choice of means of action here, hence the protection can be implemented by means of architectural-constructional solutions, as well as technical or purely IT means, e. g. access codes, chip cards, coding systems [Barta, Fajgielski, Markiewicz 2015].

Article 36a of P.D.P.A., established the right to appoint an information security administrator by the data administrator. In NDR BIB JSC, the ISA was established, whose tasks, pursuant to P.D.P.A. is to ensure compliance with the provisions on the protection of personal data, as well as to maintain a register of data files processed by the data administrator. The duties of ISA are also defined in the Regulations of the Minister of Administration and Digitization of 11 May 2015; on the manner of keeping information security administrator data filing register (Journal of Laws item 719, as amended); and on the mode and manner of performing tasks in order to ensure compliance with the provisions on personal data protection by the information security administrator (Journal of Laws item 745, as amended).

Further legal acts that regulate the issue of information protection in NDR are: the Act of 5 August 2010 on the protection of classified information (Journal of Laws No. 182, item 1228, as amended); the Act of 27 July 2001 on the protection of databases (Journal of Laws No. 182, item 1228, as amended); the Act of 27 July 2001 on the protection of databases (Journal of Laws No. 182, item 1228, as amended). Act of 18 September 2001 on electronic signature (consolidated text: Journal of Laws of 2013, item 262, as amended), but which has a lesser impact on the BIBs' activities.

Every business entity creates an information protection system which can also be defined as an information security policy. All activities in this area have several key objectives which include ensuring the confidentiality of the data to be protected, ensuring the integrity and availability of and access to public and protected data, guaranteeing the required level of data security, limiting the occurrence of various threats to information flows, ensuring the correct functioning of information processing systems, ensuring the preparedness to take action in case of possible crisis situations [Kowalewski, Ołtarzewska 2007]. The information security policy itself can be defined as a set of documents whose purpose is to define the methods and principles of protection and information security in a given institution. This collection should be consistent, precise and in compliance with the applicable law, both Polish and European [Kowalewski, Ołtarzewska 2007].

NDR BIB JSC on a daily basis face the challenge of protecting the information processed, especially the most important one, as well as that required to be protected by the above detailed legal regulations. The basic threats to information security can be divided into four groups. The first is human error, and therefore the risk of security breaches resulting from human negligence, inattention, possibly also lack of knowledge or incompetence on the part of designers, administrators or people using the system. The second group consists in broadly understood failures, i.e. unplanned and unexpected defects of hardware or software, as well as of devices whose proper operation is a prerequisite for the proper functioning of the system. The third type of threat is a natural disaster (caused by weather events, etc.), a man-made disaster (communication accidents, construction disasters), or a disturbance of information systems or related systems. The fourth group of threats is the deliberate

action of people or automated attacks against a given system, theft of equipment or resources, etc. [Pipkin 2002].

It should be stressed that in May 2018 the implementation of the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (the so-called GDPR). They concern in particular the introduction of direct liability of the data processor for breaches of the GDRP regulations, imposes additional obligations on controllers related to the reporting of violations, extends the information obligation, limits the possibility of data profiling, extends citizens' rights, imposes the need to obtain approvals for data processing, and imposes a ban on data transfer outside Europe without meeting the expected level of security standards (see [https://www.pwc.pl/pl/artykuly/2017/10-najwazniejszych-zmian-ktore-wprowadza-rodo.html, date of access: 01.01.18]).

5.2. Physical protection

Physical measures to protect databases consist mainly of restricting access to data processing equipment. As well as stopping unauthorised access, it is also necessary to protect against accidental events such as fire, flooding and other hazards. The standard, which is also used by NDR in the area of physical protection, is the investment in reinforced room structures (respectively thick doors made of heavy-duty material, wall reinforcements, server room ventilation systems, optimal layout of rooms and equipment in the case of fire, together with an alternative power supply, enabling the systems to operate even in the case of power failure or power supply interruptions).

Technical devices enabling data processing are placed in organizations which take care of information security in the premises marked as a separate security area to which only designated employees have access. What is more, usually around the protected rooms there are also protection zones with restricted access for bystanders. In the case of NDR, detailed, confidential regulations concerning the access of employees to certain premises and equipment are contained on the basis of paragraph 26 of the Bureau Security Policy regulations.

In order to be able to effectively control access to these premises, the NDR uses input/output systems, alarm systems, monitoring and security companies. In addition, in terms of physical protection, the form of security is the destruction of information carriers in such a way that it is impossible to read them. The office building of the National Debt Register has been divided for security purposes into several zones, access to which has been diversified from the point of view of the functions and tasks of individual employees.

5.3. Logical protection

Logical protection is implemented at the level of information systems. This includes various user authorisation mechanisms, which aim at limiting access to data for individuals only, data encryption mechanisms and mechanisms to ensure the overall security of information systems, i.e. protection against malware, cybercrime attacks, etc. in line with the company's policy.

The logical protection is implemented mainly through the use of IT systems. It includes data encryption mechanisms, as well as mechanisms to ensure the overall security of information systems, i.e. protection against malware, cybercrime attacks, etc. It also includes the protection of information systems against malicious software. Access restrictions may be limited, for example, by a password system, which comprises individual identification and confirmation of the user's identity in the computer system on each entry. It can be replaced even by biometric methods or supplemented by specific solutions of disposable passwords, chip cards or tokens [Angryk et al. 2005], however this level of access complication is not always applied. In fact, there is usually a different level of protection depending on the function of a person in an organization and especially the data it uses.

Amid the electronic security technologies in enterprises there are among others P3P (Platform for Privacy Preferences), a project that allows employees to set privacy protection requirements on a browser to match user preferences with the organization's security policy. Another technology with similar performance is OPS, the Open Profiling Standard, which is a standard that guarantees the secure transmission of the user profile. It is also worth mentioning the data protection generators recommended to users by the OECD. They cover all aspects of data protection, as well as privacy domains in wide area networks, integrating different national and international information protection regimes and regulations. Other technologies include cryptography, electronic signature, trust institutions, public key infrastructure, information separation, virtual private networks, multilateral security, certified systems and products [Kiełtyka 2010].

The use of data encryption in today's economic circulation is another form of action that is essential for the proper functioning of the data processor's business. In principle, two methods are used for encryption, one of which consists in the use of a symmetrical key and the other in the use of an asymmetrical key. The regulations indicate that in NDR communication with customers, the data transmitted is encrypted (paragraph 33) by means of various methods, e. g. by means of data transmission. SSL protocol or equivalent, VPN standard or certificate. The transmission of data to customers by means of electronic data carriers also requires encryption based on paragraph 34 of the regulations.

In some sections of NDR, among others, introducing IRM security measures into files created and edited in Microsoft Office programs apply. Therefore, files often set a date from which the document expires and ceases to be available, and can grant permission for specific users to print, edit, copy or open documents in general. Detailed rules are laid down in the company's internal documents.

NDR employees also have data encryption instructions which are implemented using one of the programs available on the market. Employees handling important data must have a security certificate issued by members of the Information Security Team.

For non-productive companies that provide a large part of their network services, such as NDR, the logical data protection mode is essential as a large group of customers use BIB services through websites or smartphone applications.

5.4. Procedural protection

Procedural protection refers to the maintenance of appropriate processes within the company. Procedural protection serves, generally speaking, to sanction rules on physical and logical protection. It also introduces a basic classification of data, i.e. a process that allows for an accurate determination of the level of saliency of data for the organization in order to be able to apply for them appropriate security mechanisms and a security policy. These procedures must specify, among others:

- the conditions for granting and revoking data access rights,
- data classification rules,
- rules for access to premises where data-processing facilities are located,
- minimum requirements for the application of data protection mechanisms against unauthorised access,
- principles of IT systems administration,
- a backup policy.

In the structure of the National Debt Register which employs hundreds of employees in individual departments, there are numerous security procedures in place which guarantee that access to data is granted only to the appropriate entities; paragraph 22 indicates that all employees of the Bureau who are allowed to process business information have registered authorization of the Bureau. In addition, paragraph 23 requires each employee who processes business information to keep the content and security of the business information confidential. An appropriate undertaking is signed for this purpose.

Among the procedures of securing data in NDR it is worth pointing out that it is forbidden to remove electronic data carriers containing business information from the registered office of the company without the permission of the Bureau's Management Board or Information Security Administrator (paragraph 25 of the regulations).

The ISA department in NDR receives applications from new users of data processing systems via the intranet ServiceDesk Plus application. Authorized persons log into the system, then select appropriate tabs in the system, allowing to report specific persons or possibly certain problems. Until 2014, ISA's contact with the department was based on paper forms, over time replaced by a purely electronic form which for obvious reasons is cheaper, more efficient and more environmentally friendly.

A precise set of procedures used in NDR to protect business information is contained in the Bureau's Security Policy, which is to define, among others, a list of datasets indicating the data sets used to process the programs; a description of the structure of datasets used to process the information; specification of technical and organizational measures necessary to ensure confidentiality, integrity, availability and accountability of the data processing; scope of employee responsibility for data processing; description of the applied security measures applied; principles for dealing with threats to the security of the IT system and data processing; principles of conducting training courses.

In paragraph 27 of the regulations, on the other hand, a delegation for the development and implementation of the IT System Management Instructions in the procedures for granting authorization to process data and record such instances together with the identification of persons responsible for these activities was included; methods and means of authentication applied in the company and procedures related to them; procedures for creating backup of data sets; rules for storing and destroying electronic data carriers; methods of protecting systems

against external, harmful software; ways to protect the system against loss of confidentiality, integrity, accountability, availability, etc.

According to the internal regulations of NDR, data contained in databases can be made available only to authorized users or systems, which results, firstly, from the legal requirements and the laws discussed earlier, and secondly, from the need to ensure information security within the organization itself. To ensure the confidentiality of data it is necessary to ensure that they are secure at every appropriate stage of the processing process, from restricting access to devices to specific users only, to controlling access to data-processing systems, to ensuring transmission security, backups and even prints containing data or images from data displays. Due to the importance and complexity of the process, the data processing policies and procedures, as well as the documentation related to them, play a key role in ensuring confidentiality of data.

In the internal circulation of NDR there are several groups of documents whose workflow is covered by different procedures. These are system documents (policies, declarations), operational, normative, financial and accounting documents and records. Documents of the highest importance shall be developed and stored by the Quality Management System Board's representative. The lower-level documents of the Information Security Management System are stored by the Information Security Team.

In general, the lead documents shall be kept in paper and electronic form. Operational documents, which are the basis for the business functioning of the organization, are created and updated by the process/ product owners. Updates and changes in documents from the above mentioned groups require the approval of the President of the NDR Management Board.

Each time the company's documents are created, it is required to take the legal requirements, standards and internal legislation as well as the requirements of the parties concerned into account. The procedures of NDR therefore first require the appropriate arrangements and approvals with the parties or stakeholders. Approval and publication is further required. In the case of the ISMS's lead documents, this is done by the Senior Management, while other documents are approved by the directors or managers responsible for the specific area to which the document applies. Approval of paper documents shall require a signature on the cover page and, optionally, a stamp in the name of the person concerned. The electronic documents shall, however, be approved by a favourable opinion on them and the decision to publish them.

Paper documents must be stored in lockable cabinets if they are to be stored on paper. Electronic documents are stored in specific locations such as an e-mail system, personal network resource, shared network resources, public folders, SharePoint

6. Conclusion

Business Information Bureaux are entities for which the issue of information security is of vital importance. In today's reality, information on debt and data on private documents are extremely important in order to protect various entities from dishonest or insolvent contractors, thus stabilising the economic cycle.

The aim of the article has been achieved. The concept of business information has been characterized on the basis of literature review. Its specific features have been identified and a theoretical model of the information security system in the business information office has been proposed. Then, based on the analysis of the actual case of the company, NDR BIB JSC, the legal and organizational requirements for business information offices are presented, as well as the solutions applied in their field in practice. The presented analysis allows us to conclude that the collection, storage and disclosure of business information requires a complex security system. It seems that the activities of the entities discussed in this article can be classified as the most restrictive, regulated by Polish law.

Issues related to business information processing security management are an interesting area for further research, especially in the context of the development of big data technology and machine learning.

Bibliography

Angryk R., Bandosz M., Hoffmann M.R., Olejniczak W., 2005, *E-gospodarka*, [w:] *Inżynieria systemów informatycznych w e-gospodarce*, eds E. Kolbusz, W. Olejniczak, Z. Szyjewski, Polskie Wydawnictwo Ekonomiczne, Warszawa, pp. 15-45.

Barta J., Fajgielski P., Markiewicz R., 2015, *Ochrona danych osobowych. Komentarz*, Wolters Kluwer Polska, Warszawa.

Bekas M., 2011, *System wymiany informacji gospodarczych w Polsce*, Studia i Prace Kolegium Zarządzania i Finansów, z. 109, pp. 7-15.

Bertino E., 1998, *Data security*, Data & Knowledge Engineering, vol. 25, Issues 1-2, March pp. 199-216.

Białek T., Marzec A., 2011, *Ustawa o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych. Komentarz*, Wolters Kluwer Polska, Warszawa.

Colwill C., 2009, *Human factors in information security: The insider threat – Who can you trust these days?*, Information Security Technical Report, vol. 14, Issue 4, November, pp. 186-196.

https://krd.pl/, data dostępu: 10.l2.17.

https://www.pwc.pl/pl/artykuly/2017/10-najwazniejszych-zmian-ktore-wprowadza-rodo.html, date of access: 01.01.18.

Humphreys E., 2008, *Information security management standards: Compliance, governance and risk management*, Information Security Tech. Report, vol. 13 no. 4, pp. 247-255, November.

Kiełtyka L., 2010, *Systemy informatyczne zarządzania informacją*, [w:] *Informatyka gospodarcza 3*, J. Zawiła-Niedźwiecki, K. Rostek, A. Gąsiorkiewicz (eds), Wydawnictwo C.H. Beck, Warszawa, pp. 475-506.

Kowalewski M., Ołtarzewska A., 2007, *Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego*, Telekomunikacja i Techniki Informacyjne, nr 3-4, pp. 3-9.

Koziej S., 2011, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja,* Polityczno-strategiczne aspekty bezpieczeństwa, Bezpieczeństwo Narodowe, nr 18, pp. 19-39.

Liginlala D., Simb I., Khansac L., 2009, *How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management,* Computers & Security, vol. 28, Issues 3-4, May-June, pp. 215-228.

Nowak A., Scheffs W., 2010, *Zarządzanie bezpieczeństwem informacyjnym*, Wyd. AON, Warszawa.

Oleński J., 2001, *Ekonomika informacji. Podstawy*, Polskie Wydawnictwo Ekonomiczne, Warszawa.

Pipkin D.L., 2002, *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, Wydawnictwo Naukowo-Techniczne, Warszawa.

PN ISO/IEC 27001:2007, 2007, *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, PKN.

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

Sopińska A., 2004, *Leksykon zarządzania*, Difin, Warszawa.

Szustak G., 2014, *Informacja o kredytobiorcy – zasadnicza przesłanka bezpieczeństwa banku*, Studia Ekonomiczne – Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach, nr 171, pp. 65-83.

Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. nr 182, poz. 1228 ze zm.); Act of 5 August 2010 on the protection of classified information (Journal of Laws no. 182, item 1228 as amended).

Ustawa z 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych, tekst jedn.: Dz. U. 2014 r., poz. 1015 ze zm.; Act of 9 April 2010 on fascilitating of business information and exchange of economic data (consolidated text: Journal of Laws of 2014, item 1015 with as amended).

Ustawa z 14 lutego 2003 r. o udostępnianiu informacji gospodarczych (Dz. U. nr 50, poz. 424 ze zm.); Act of 14 February 2003 on fascilitating of business information (Journal of Laws no. 50, item 424, as amended).

Ustawa z 18 września 2001 r. o podpisie elektronicznym (tekst jedn.: Dz. U. z 2013 r., poz. 262 z późn. zm.); Act of 18 September 2001 on electronic signature (consolidated text: Journal of Laws of 2013, item 262, as amended).

Ustawa z 27 lipca 2001 r. o ochronie baz danych (Dz. U. nr 128, poz. 1402 ze zm.); Act of 27 July 2001 on the protection of databases (Journal of Laws no. 128, item 1402 as amended).

Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2016 r., poz. 922 ze zm.); Act of 29 August 1997 on the protection of personal data (consolidated text: Journal of Laws 2016, item 922, as amended).

Velumadhava Raoa R., Selvamanib K., 2015, *Data Security Challenges and Its Solutions in Cloud Computing*, Procedia Computer Science, vol. 48, pp. 204-209.

Wyrębek H., 2012, *Bezpieczeństwo w zarządzaniu informacją na poziomie systemów informatycznych*, Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Administracja i Zarządzanie, nr 95, pp. 463-470.

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI GOSPODARCZYCH NA PRZYKŁADZIE KRAJOWEGO REJESTRU DŁUGÓW BIURA INFORMACJI GOSPODARCZEJ SA

Streszczenie: Celem artykułu jest scharakteryzowanie specyfiki informacji gospodarczych i problematyki zapewnienia im bezpieczeństwa na przykładzie przedsiębiorstwa, jakim jest biuro informacji gospodarczej. Analizie poddano Krajowy Rejestr Długów Biuro Informacji Gospodarczej SA, które jest pierwszym i jednym z największych tego typu podmiotów funkcjonujących w Polsce. W artyfkule omówiono w pierwszej kolejności specyfikę informacji gospodarczych jako szczególnego typu informacji, regulowanego dotyczącą ich ustawą. W dalszej części dokonano analizy funkcjonowania systemów i procedur ochrony informacji w biurze informacji gospodarczej. Przedstawione zostały zasady ochrony logicznej, fizycznej oraz proceduralnej, które informacjom gospodarczym w przedsiębiorstwie pozwalają zapewnić należyte bezpieczeństwo. Analiza rzeczywistego przypadku biznesowego pozwoliła ukazać, w jaki sposób w praktyce wdrożone zostały wymagania nałożone na biura informacji gospodarczej w zakresie systemu zarządzania bezpieczeństwem informacji.

Słowa kluczowe: informacja gospodarcza, biuro informacji gospodarczej, ochrona, bezpieczeństwo informacji.