INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 1(47) • 2018
ISSN 1507-3858
e-ISSN 2450-0003

Robert Kucęba, Grzegorz Chmielarz
Czestochowa University of Technology
e-mails: robertk@zim.pcz.pl; grzegorz0101@gmail.com

ISSUES OF PERSONAL DATA MANAGEMENT IN ORGANIZATIONS – GDPR COMPLIANCE LEVEL ANALYSIS

PROBLEMATYKA ZARZĄDZANIA BEZPIECZEŃSTWEM DANYCH OSOBOWYCH W ORGANIZACJACH – ANALIZA STOPNIA ZGODNOŚCI Z RODO

DOI: 10.15611/ie.2018.1.05

Summary: The paper presents the issues of information and personal data security management in organizations. The authors include in it an analysis of breaches to personal data security in organizations as a vital factor that conditions the necessity to improve the previously applied solutions in this area. Additionally, the paper contains analyses concerning the preparation level of organizations to ensure compliance with the General Data Protection Regulation (GDPR) which is coming into force. The paper constitutes a cognitive query in the scope of the subject matter defined in its title.

Keywords: personal data, personal data protection, personal data security breaches, GDPR.

Streszczenie: W artykule przedstawiono problematykę zarządzania bezpieczeństwem informacji oraz danych osobowych w organizacjach. Zawarto w nim analizę przypadków naruszenia bezpieczeństwa danych osobowych w organizacjach jako istotnego elementu warunkującego konieczność usprawnienia istniejących w organizacjach rozwiązań w tym obszarze. Ponadto w artykule przedstawiono analizy dotyczące stopnia przygotowań organizacji do zapewnienia zgodności z wchodzącym w życie Ogólnym Rozporządzeniem o Ochronie Danych Osobowych. W całości artykuł ma charakter kwerendy poznawczej z zakresu tematyki określonej w tytule.

Słowa kluczowe: dane osobowe, ochrona danych osobowych, naruszenie bezpieczeństwa danych osobowych, RODO.

1. Introduction

The issues of ensuring security of information resources in heterogeneous organizations is a vital element of enterprises' functioning in the current economic reality, which is to a large extent driven by the growth in the number of attacks aimed

at the information repositories of these organizations. However the information security of an entity (a human being or organization) means not only the ability to acquire good quality information but also the protection of already possessed information against its loss [Korzeniowski 2012, s. 147]. In the opinion of J. Stańczyk, "*security is a state of confidence, peace, guarantee and its feeling, as well as the lack of threat and protection against danger"* [Stańczy 1996]. W. Šmid believes that "*security is a situation characterized by the lack of risk, e.g. in investments, strategic plans, tangible assets and human resources*". T. Łoś-Nowak states that the concept of security itself is difficult to define as it does not only constitute a state that is possible to define at a given place and time, but is a dynamic process that changes over time [Łoś-Nowak 2003, s. 37-38]. Referring purely to the subject matter defined in the paper's title, R. Borowiecki and M. Kwieciński state that information security means just "*information defence, which consists in preventing and hindering the acquisition of data on the physical nature of the current and planned state of affairs and phenomena in their own functioning space and hindering the introduction of information entropy introduction into communications, and physical destruction into data carriers*" [Borowiecki, Kwieciński 2003]. M. Laskowski turns his attention to the definition of information security in informatics, where it might adopt two meanings: **security** – referring to data protection in networks and computer systems and **safety –** the resilience of those networks and systems to failures, both resulting from their unreliability, as well as driven by the impact of external factors regardless of their origin. A computer system might be considered safe if its users may expect that information permanently introduced into the system will not be lost, modified or used in an unauthorized or accidental manner [Laskowski 2013, p. 15-16]. Attacks aimed at unauthorized access to private information and personal data concern all systems that operate being connected to the global network – the Internet. Threats to the private personal data of users may come in various forms. Apart from unauthorized access they also include equipment failures, and accidental removal or modifications by unauthorised persons. Personal data breaches constitute a significant threat to the continuity of organizations' operation, therefore it appears appropriate that proper policies and procedures are implemented that regulate the security management issues of processed personal data. Such a necessity is determined by the number and scope of impact of personal data security breaches that occur on a global scale. In 2016 these included the personal data theft of Yahoo users, which concerned about 1 billion users and the MySpace website where the personal data of 427 million users were stolen. In Poland a well-known example is the personal data disclosure of Uber users, which concerned about 70 thousand users. In the United States in 2017 the data of 143 million EquiFax website users were stolen and in 2018 the personal data theft of 800 thousand Swisscom clients were subject to theft[1]. One of the reasons behind such occurrences is the low level of measures applied by organizations to

[1] https://www.computerworld.pl/news/Nie-ma-firmy-za-malej-na-bezpieczenstwo,409986.html (access: 26.04.2018).

ensure the security of the personal data they process. As a result, the European Union decided to update and radically modify legislation in this area, introducing a new regulation that unites and unifies information and personal data protection issues in all organizations where personal data processing occurs. On 25 May 2018 a new EU **General Data Protection Regulation**, commonly called GDPR, became effective. Unfortunately, as the results of a survey by ECM Insights demonstrate, only 25% of large enterprises believe that they are ready to implement the regulation. It should also be stressed that according to the results of the aforementioned survey almost a half, that is as many as 45% of the companies have not yet developed a strategy that would ensure compliance with new EU requirements yet[2]. Therefore, the goal of this paper is to analyse the threats in the area of information and personal data protection management in organizations, being a direct result of new IT technologies' development. Based on literature study the authors present statistics concerning breaches of personal data security in organizations – on a global scale. Additionally, the paper includes an analysis of the level of organizations' readiness to ensure compliance with the GDPR and also presents the financial barriers that constitute one of the main reasons for delays in the GDPR's implementation in organizations. The research method used to obtain data used in the analyses was an extensive literature research that provided secondary data to demonstrate changes in the area of data security management which are the outcome of the GDPR introduction. Due to the topicality of the subject matter, the paper may prove to be a valuable source of information for organizations that are implementing the GDPR in their information security systems.

2. Challenges for ensuring personal data protection

The creation of the General Data Protection Regulation – GDPR – is the outcome of advances in information technologies development, which are implemented and utilized on a large scale, and resulted in a substantial growth in the amount of personal data that is processed in organizations within their IT systems. Applying new tools allowed data processing to reach unprecedented dimensions. With the Internet being commonly available and utilized in operations of a great number of organizations, the amount of data is growing rapidly; this refers to private data that are currently available on the market. For example, currently within one or two days as much data are produced as globally produced up to 2003[3]. Therefore the growth in the amount of processed data produces new challenges for organizations with reference to managing properly the personal data they possess and ensuring its appropriate protection. The acquired and gathered information that can be analysed constitutes a considerable economic

[2] https://avlab.pl/pl/ecm-insights-2017-tylko-25-europejskich-przedsiebiorstw-jest-gotowych-na-rodo (access: 26.04.2018).

[3] http://www.giodo.gov.pl/487/id_art/9146/j/pl/ (access: 26.04.2018).

value. For instance, the value of EU citizens data in 2011 amounted to EUR 315 billion. It is expected that by 2020 this can increase up to almost EUR 1 billion per year. In 2013 the value of data stolen globally was USD 8 billion[4]. The consequence of this state of affairs is the increased awareness of Internet users regarding the importance of private information on users being managed properly by organizations. The research that analyses the user trust level towards secure personal data management in organizations demonstrates a significant decrease in this area. According to the results of the research conducted in Germany in 2011-2017, only about 20% of the respondents believed that their private personal data used on the Internet were secure, while the great majority of them (78%) stated that their personal data were poorly secured. For reference, in 2011 about 40% of the respondents believed that their data present in IT systems were processed safely, and 55% of them believed they were rather unsafe. Additionally, it needs to be pointed out that the lowest level of trust in respect of their private data security was declared by German Internet users in 2014, when it amounted to 13%. This level increased to 21% in 2016, which could constitute one of the vital incentives for introducing by the European Parliament and the Council, the General Data Protection Regulation[5]. The results of the presented secondary research (*Data Security in Germany*) are shown in Figure 1.

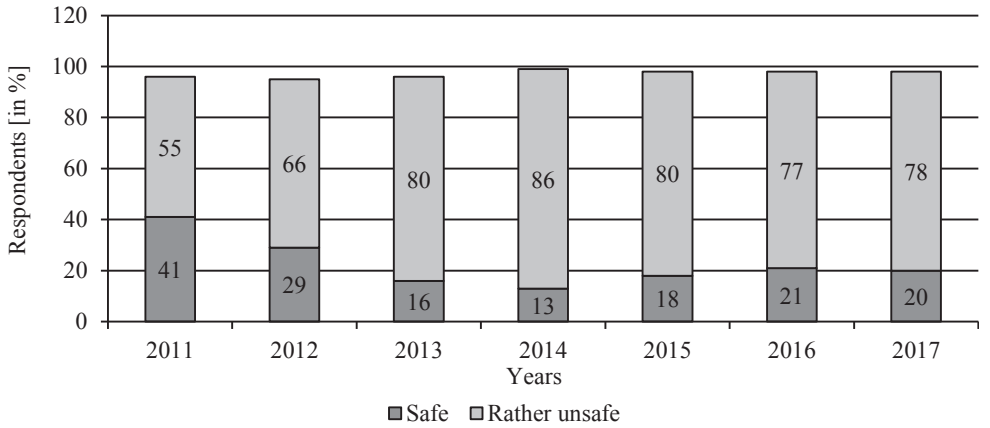

Fig. 1. Personal data security level in Germany in 2011-2017

Source: own elaboration based on: https://www.statista.com/statistics/448431/perception-of-online-data-security-in-germany/ (access: 27.04.2018).

Another widespread problem following the growth in the amount of processed personal data are breaches to personal data security and such data disclosures

[4] http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/ (access: 26.04.2018).

[5] https://www.statista.com/statistics/448431/perception-of-online-data-security-in-germany/ (access: 26.04.2018).

resulting from unauthorised access to it. A considerable growth in the number of such occurrences is the outcome of the common utilization of digital forms of personal data by organizations and the large interdependence between their use and the efficiency of these entities operations. With this in mind, a key aspect becomes how to manage security of the information systems in organizations. Although the information technology itself may in fact increase efficiency of information management, particularly when implementing new solutions will improve the processes of information, its acquisition, gathering and storing, processing, emission and making it available, still one of the most essential factors that condition the successful implementation of the solutions of information management support systems is the "organizational climate of the organization" and its information culture [Jelonek, Chomiak-Orsa 2011, s. 97]. Personal data security breaches regarding private persons actually had already occurred before the processing in the digital form began, yet the widespread use of such large amounts of data, as well as the growing importance of unauthorised access incidents brought a new dimension to the issue of proper personal data management and ensuring its protection. In a global perspective, identity theft represented the most prevailing type of personal data security breaches in 2016, accounting for 59% of all recorded incidents of this kind. The most famous one concerned stealing information on private users from Yahoo in 2013, as a result of which hackers gained access to the personal data of over 1 billion account owners of this website. Another such case occurred a few months later and resulted in disclosing over 500 million data records of website users[6]. As many as 229 serious breaches to data security were recorded in Europe in 2004-2014. However, already in the first half of 2017, 918 personal data security breaches occurred globally, majority of them being again identity thefts, that is access to the private personal data of users – 74%. Personal data were also used to gain access to finances in 13% of cases, 6% represented cases of accessing accounts and access to existential data. An impediment for data owners constituted by the unauthorised access to personal data in just 1% of cases. The data on personal data security breaches are aggregated in Figure 2.

In the United States the number of breaches to personal data security reached the highest ratio in 2017, when almost 170 million personal data records were revealed and the total number of personal data security breaches amounted to 1579. The sector most affected by personal data thefts was the business sector, where 91.3% of all personal data disclosure occurrences took place. This is also the reason why cybercrime results in the highest average cost of losses in the financial sector in the USA. In 2015 cybercrime led to losses in this sector that amounted to about USD 28 million. The most popular types of attacks aimed at personal data thefts used malicious software in the form of viruses, worms and Trojans. The situation is exacerbated by the fact that more and more frequently, the information resources of

[6] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (access: 26.04.2018).

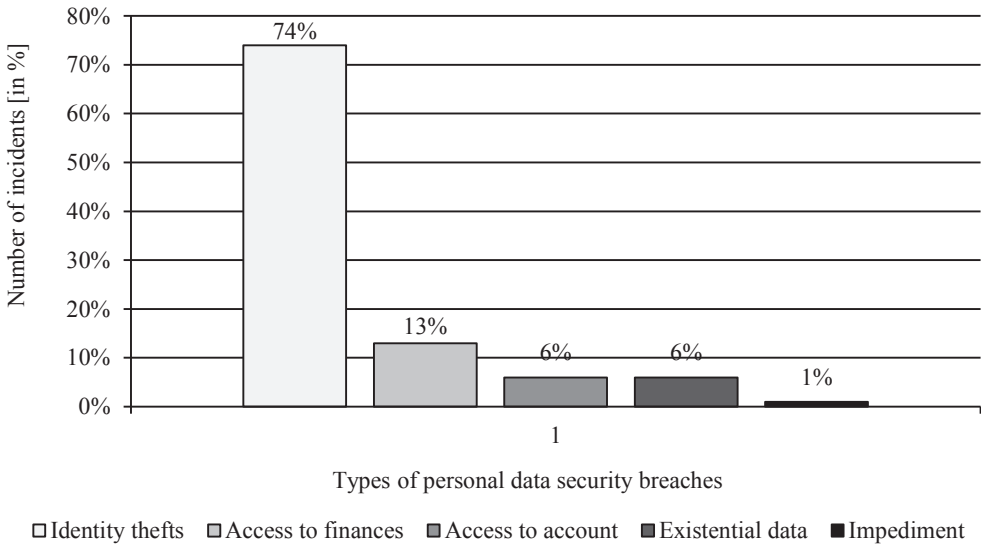

Fig. 2. Types of personal data security breaches globally in the first half of 2017

Source: own elaboration based on: https://www.statista.com/statistics/329593/frequency-share-incident-classifiaction-patterns/ (access: 27.04.2018).

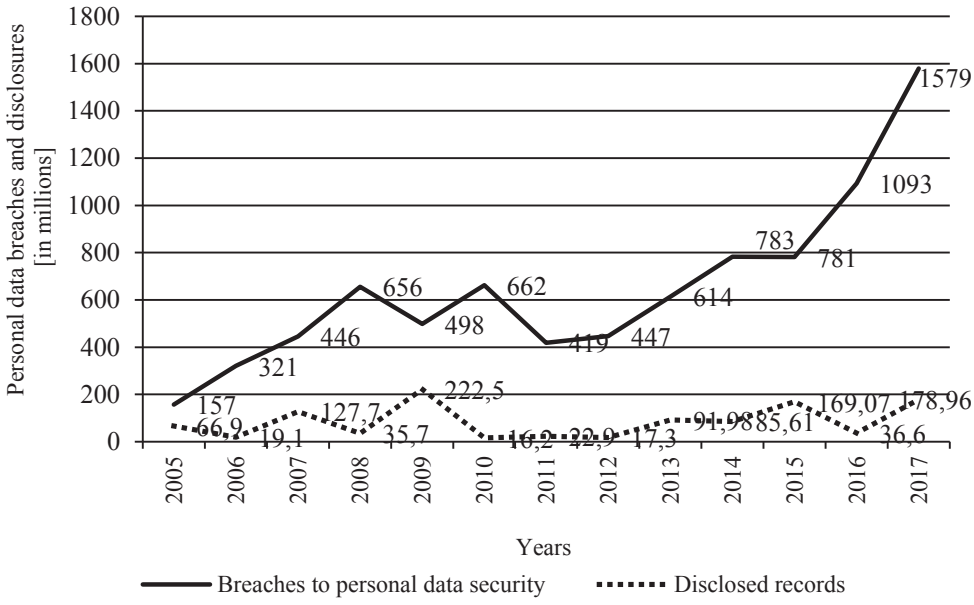

Fig. 3. Statistics on personal data breaches and disclosures in the United States in 2005-2017

Source: own elaboration based on: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (access: 26.04.2018).

organizations are attacked with the use of malicious software from inside the organization, which proves that particular stress should be placed on proper information security management in organizations. Statistically, attacks of this type are also the most time-consuming in respect of removing their effects, on average this takes almost 69 days[7]. The statistics on personal data breaches and disclosures in the United States in 2005-2017 are presented in Figure 3.

It needs to be stressed that the presented examples of the data privacy breaches of Internet users explain that previously valid legal solutions in the area of personal data protection management did not constitute satisfactory protection in this field. This stimulates the necessity to update the regulations in this area. Such a measure in the European Union was the adoption of the General Data Protection Regulation, which became effective on 25th May 2018. The regulation introduces a number of significant changes that are meant to improve the efficiency of the personal data processed in organizations.

3. Evaluation of GDPR implementation in organizations

The dynamic development of new technologies has led to a tremendous increase in the amount of processed data. However, the legal regulations in force regarding personal data protection management have not kept up with the pace and scale in the area of personal data processing in organizations. For example, the laws in force in the European Union that regulate the issues of personal data protection were introduced in the form of the Directive 95/46/WE in 1995. This directive was implemented in the national laws of the EU member states, which resulted in adopting in Poland the Law on Personal Data Protection of 29 August 1997 (Dz. U.02.101.926), amended several times, last amended on 28 June 2016 (Dz. U. z 2016 item 922). As the EU directives aim at unifying the law in the whole of the EU, the implemented solution resulted in a considerable differentiation of the regulations concerning personal data protection in the individual member states of the European Union, and hindered the operations of organizations that process personal data. Additionally, respecting the rights of the persons concerned also became more problematic [Dmochowska, Zadrożny 2016, s. 2]. At the same time, the newly introduced law regulations did not keep up with the changes in the process of personal data processing, which was mainly driven by the development of new information technologies. Therefore, following the negotiations between the European Parliament and the European Council, new regulations in the area of personal data protection were adopted in the European Union, namely the Regulation of the European Parliament and of the Council 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the Directive 95/46/WE – the GDPR. The regulation

[7] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (access: 26.04.2018).

25 May 2016, however, a two-year transitional period was introduced so as to allow the organizations functioning in the member states to adjust their policies and procedures to the provisions of the GDPR. As the GDPR was adopted in the form of a regulation, not a directive, which means that it will have a direct application in all the EU's member states and does not require to be implemented by a Polish law. However, the Ministry of Administration and Digitalization drew up a working draft of a new law on personal data protection, which is supposed to adjust Polish legislation to the GDPR requirements. However it needs to be pointed out that the application of the GDPR is not limited exclusively to organizations physically located in the territory of the European Union. The provisions of the new regulation concern all economic entities that through their websites offer their products or services to EU customers. This is a significant change compared to previously valid regulations, which according to the interpretations of judicial authorities applied only to organizations with registered offices in a given EU member state. As a result, work started to ensure compliance of personal data protection process, convergent with provisions of the GDPR, by organizations all over the world, including the United States and Japan. The adjustment level of user personal data management procedures was the subject of research in 2016-2017, by amongst others, PwC. According to the results of the survey conducted among the senior staff in companies in Great Britain, the USA and Japan, 11% of the respondents stated that operational work had been completed in their organizations, which is an increase of almost 100% compared to the previous year, where such an answer was given by only 6% of the respondents. Only 7% of the companies stated that preparations to ensure compliance with the GDPR had not started yet, which is a significant drop from the 23% recorded in the survey in 2016. However it should be pointed out that considerable differences in the analysed area still exist. About a third (36%) of the surveyed companies only recently started the process of evaluating their compliance with the GDPR requirements, which means that by 25 May 2018 their activity would not be fully compliant with the new regulations, which in turn may lead not only to losing contracts in Europe, but also the danger of facing court proceedings and financial penalties stipulated in the new regulation for not complying with the requirements to ensure the proper protection for processed personal data. The aforementioned data are presented in Figure 4.

Compared to Great Britain and Japan, American companies recorded the largest progress in the scope of adjusting the personal data protection management procedures implemented in these organizations to the requirements of the GDPR. Almost a quarter (22%) of companies covered by the survey in the United States declared that preparations to comply with the GDPR had been completed. In Great Britain this concerns only 8% of the companies, and in the case of Japan merely 2% of them[8]. The

[8] https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html (access: 28.04.2018).

aggregated data concerning the GDPR compliance in these countries are presented in Figure 5.

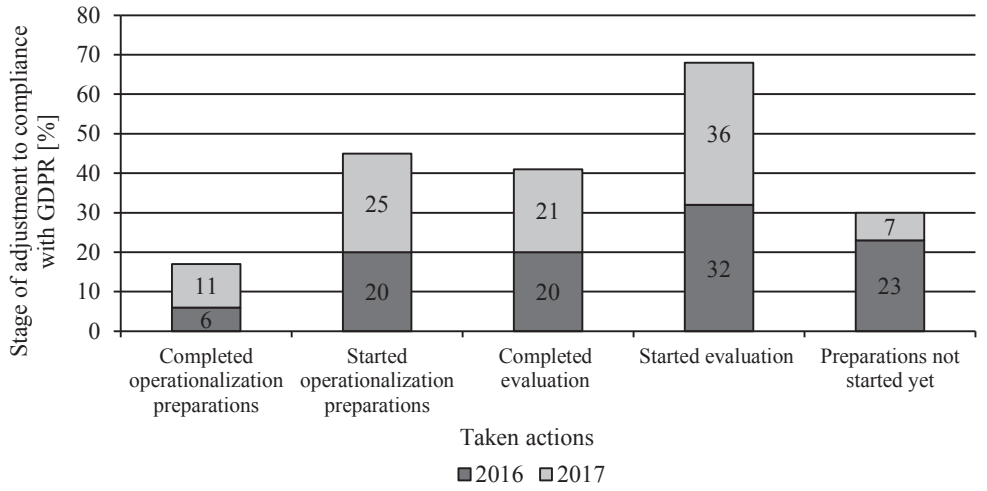

Fig. 4. Stage of preparations to ensure compliance with GDPR in 2016-2017, in Great Britain, Japan and the USA

Source: own elaboration based on: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html (access: 28.04.2018).

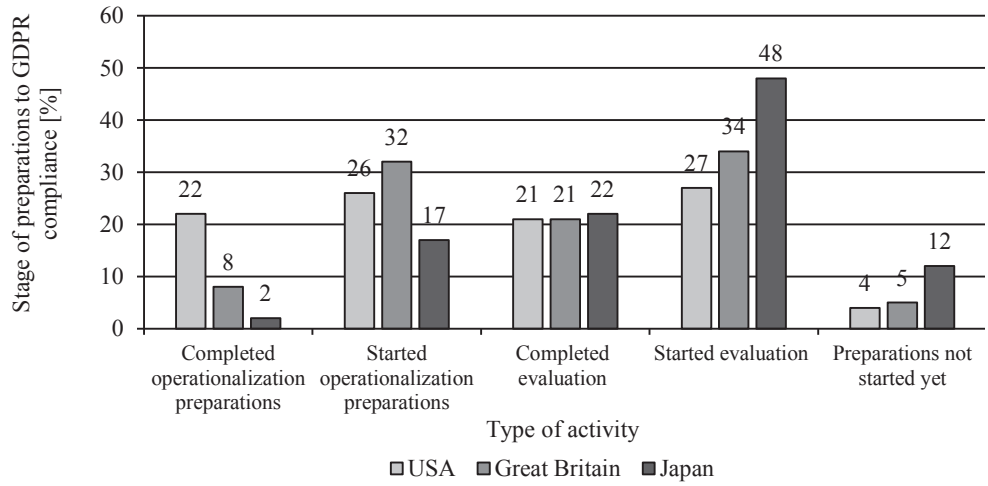

Fig. 5. Stage of preparations to ensure compliance with GDPR – companies in Great Britain, Japan and the USA

Source: own elaboration based on: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html (access: 28.04.2018).

The research conducted by other market research companies also demonstrates that in a number of cases, organizations will not manage to adjust personal data protection management procedures to the new legislation on time. For example, the authors of the report "Cybersecurity market research in Poland in 2017" indicate that representatives of every fifth large and medium-sized company operating in Poland are convinced that the GDPR does not concern their organization and they do not have to make any adjustments in this scope. It is worth pointing out that every fourth company had not encountered the term GDPR before (November 2017)[9]. According to the survey conducted by SpiceWorks, as many as 57% of companies had not included in their budgets any financial resources to implement the new EU regulations on personal data protection. What is even worse, in numerous cases preparations to the GDPR had not been even acknowledged in organizations' budgets. The results of the survey conducted by another market research company, Alert Logic, despite the fact that the wording of the GDPR is familiar to 77% of the European enterprises, merely in 5% of them the implementation of necessary changes will have been completed before the regulation becomes effective[10].

One of the barriers that influence the allocation of financial resources in organizational budgets destined to adjust their personal data management processes seems to be the high costs of such actions. As shown by the results of the report by Deloitte, the expenditures of organizations to ensure the GDPR compliance are considerably diversified. Over a third of the survey participants (39%) spent or are going to spend less than EUR 100 thousand to adjust to the new regulations and 15% declare expenditures exceeding EUR 5 million. According to the report, organizations that employ fewer than 10 000 employees are going to spend over EUR 2.5 million to achieve compliance with the GDPR, and those that employ over 50 000 employees will spend less than EUR 250 000 to implement its provisions[11]. The research conducted by PwC also indicates the significant cost that needs to be incurred in order to ensure compliance with the GDPR provisions. According to the data by this company, among the organizations that have already completed their GDPR compliance preparations, 88% spent over USD 1 million for this purpose and 40% declared a spend for this purpose of over USD 10 million. The distribution of expenditures does not depend on the company's size. The size of budget allocated for ensuring compliance with the GDPR reflects a cross-cutting approach of many of the companies to complete the preparations in this area of their functioning[12].

Similar research concerning the size of budget necessary to adjust the procedures of managing personal data security in organizations was also conducted by the

[9] http://www.cyberdefence24.pl/znaczenie-bezpieczenstwa-danych-w-firmie-wyniki-badania-rynku-cyberbezpieczenstwa-w-polsce-2017-analiza (access: 29.04.2018).

[10] https://www.computerworld.pl/news/Ponad-polowa-firm-nie-zaplanowala-jeszcze-budzetu-na-wdrozenie-RODO,409418.html (access: 29.04.2018).

[11] https://www2.deloitte.com/pl/pl/pages/press-releases/articles/wiekszosc-firm-wciaz-zwleka-z-wdrozeniem-RODO.html (dostęp: 29.04.2018).

[12] https://www.itbusinessedge.com/articles/how-to-create-your-gdpr-budget.html (dostęp: 29.04.2018).

consulting company SIA Partners. The research involved European companies from the FTSE 100 index (Financial Times Stock Exchange 100). The results of this research demonstrate that the cost of adjusting the previous regulations in the area of personal data processing to make them compliant with GDPR regulations is on average EUR 17 million[13]. Not all the companies from the FTSE 100 index will have to incur identical financial expenditures, as the compliance process itself depends on factors such as: size, IT system complexity level, number of products and service lines. However, some regularities are noticeable with reference to large organizations that employ over 5 thousand employees. In this case a dependence occurs between implementation costs and organization size, being the result of the growth in the number of factors that have to be considered in connection with ensuring compliance with the GDPR, and whose number grows together with the size of organization. In the case of organizations that already employ over 5 thousand employees, the size of the budget allocated to adjust the organization to the GDPR requirements is considerable. The minimum and average cost of the GDPR implementation in the case of the FTSE 100 index companies is fixed in the enterprise size section, calculated per one employee, and amounts to approximately EUR 400-500 in all the sectors[14]. Data concerning the size of financial expenditures allocated to ensure the GDPR compliance depending on the organization's size are presented in Figure 6.

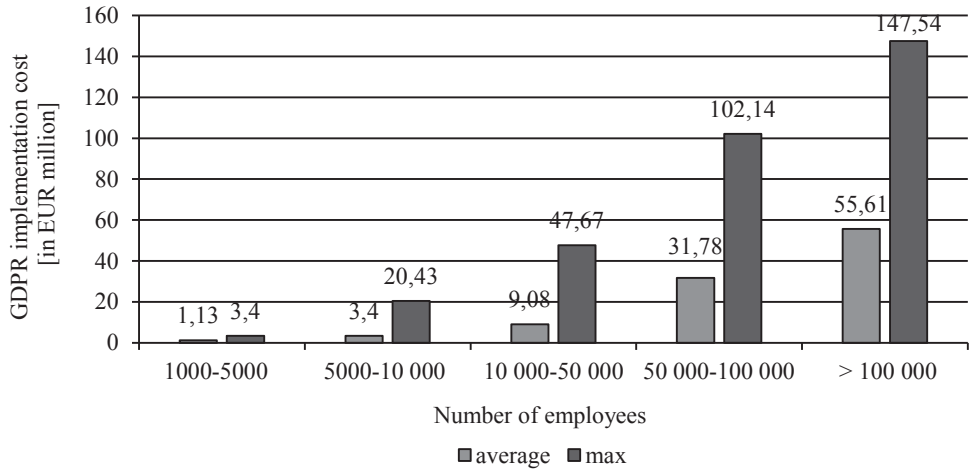

Fig. 6. Size of financial expenditures allocated to ensure GDPR compliance depending on organization's size

Source: own elaboration based on: http://en.finance.sia-partners.com/20180115/preparing-gdpr-why-you-need-ps15m-or-ps300-ps450-employee-average-implement-gdpr (access: 29.04.2018).

[13] http://en.finance.sia-partners.com/20180115/preparing-gdpr-why-you-need-ps15m-or-ps300-ps450-employee-average-implement-gdpr (dostęp: 29.04.2018).

[14] http://en.finance.sia-partners.com/20180115/preparing-gdpr-why-you-need-ps15m-or-ps300-ps450-employee-average-implement-gdpr (access: 29.04.2018 r.)

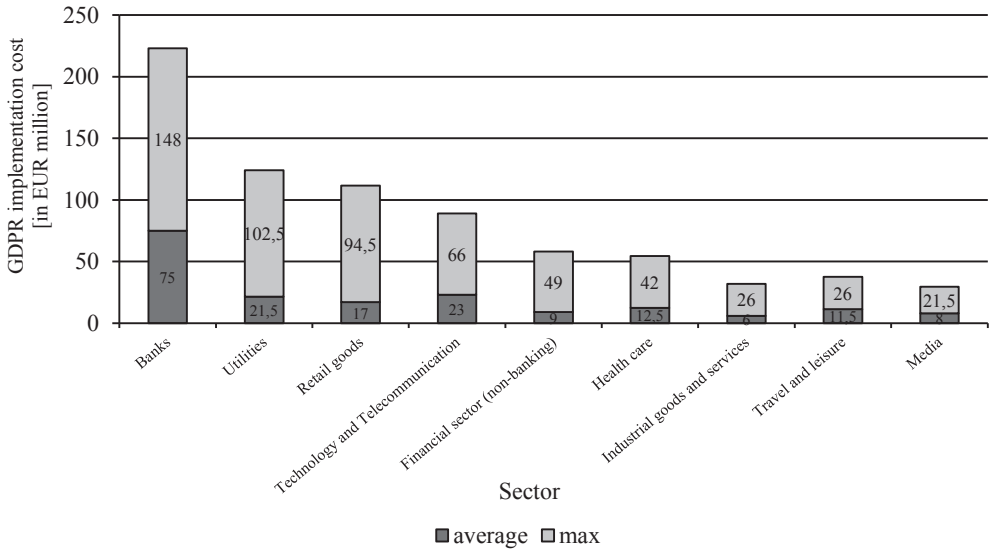

Fig. 7. GDPR implementation cost in various economy sectors

Source: own elaboration based on: http://en.finance.sia-partners.com/20180115/preparing-gdpr-why-you-need-ps15m-or-ps300-ps450-employee-average-implement-gdpr (access: 29.04.2018).

While comparing the GDPR implementation cost in various areas of the economy on the basis of the research by SIA Partners, one can notice that the highest cost of ensuring compliance with the GDPR is incurred by the financial sector institutions. On average, banks will spend for this purpose EUR 75 million, and a maximum of even EUR 150 million. Expenditures of other sectors will amount on average to EUR 17-21 million in the case of the utilities, retail goods and technology and telecommunication sectors.

Expenditures of all the other sectors will to amount between EUR 6 and 12 million[15]. The data concerning the GDPR implementation costs in various economy sectors are presented in Figure 7.

4. Conclusion

The development of information technologies and the possibility of unconstrained access to the Internet, as well as its widespread application in the operations of organizations, result in generating tremendous amounts of data. Currently, large amounts of information of private nature are present on the market. Acquired and stored information, after being subject to analysis, constitutes a significant economic value – in line with the total value of the organization, which brings new challenges

[15] *Ibidem*.

in the area of personal data management and ensuring its proper protection. The research conducted among the users demonstrate a significant decrease in the trust towards their personal data protection by organizations. This view is largely influenced by breaches to personal data security and the resulting personal data disclosures, which are the effect of unauthorized access. A significant growth in the number of such incidents is driven by the fact that organizations utilize digital versions of personal data. At the same time, legislative measures in the area of personal data protection do not consider the scale on which personal data is currently processed in organizations. Therefore proper steps have been taken by the European Union in order to address the problem which has resulted in the introduction of the General Data Protection Regulation – GDPR. Unfortunately, on the basis of the conducted analysis, it can be concluded that many organizations were relatively late to start their preparations to comply with the requirements of the GDPR, which means that as of 25 May 2018, their activity is not fully compliant with the new regulations. Thus it can be stated that one of the barriers in this area which determines the allocation of financial resources in organizational budgets for the purpose of adjusting their personal data protection processes to the requirements of the GDPR, seems to be the high cost of such actions.

Bibliography

Borowiecki R., Kwieciński M., 2003, *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze, Kraków.

Dmochowska A., Zadrożny M., 2016, *Unijna reforma ochrony danych osobowych. Analiza zmian*, Wydawnictwo C.H. Beck, Warszawa.

Jelonek D., Chomiak-Orsa I., 2011, *Nadmiar informacji. Próba identyfikacji problemu w małych i średnich przedsiębiorstwach,* Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 217, Wrocław.

Korzeniowski L.F., 2012, *Podstawy nauk o bezpieczeństwie*, Warszawa.

Laskowski M., 2013, *Współczesne technologie informatyczne. Techniki ochrony informacji*, Politechnika Lubelska, Lublin.

Łoś-Nowak T., 2003, *Bezpieczeństwo*, [w:] A. Antoszewski i R. Herbut (red.), *Leksykon politologii*, Alta 2, Wrocław.

Stańczy J., 1996, *Współczesne pojmowanie bezpieczeństwa*, ISP PAN, Warszawa.

Internet sources

http://en.finance.sia-partners.com/20180115/preparing-gdpr-why-you-need-ps15m-or-ps300-ps450-employee-average-implement-gdpr (dostęp: 29.04.2018).

http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/ (access: 26.04.2018).

http://www.cyberdefence24.pl/znaczenie-bezpieczenstwa-danych-w-firmie-wyniki-badania-rynku-cyberbezpieczenstwa-w-polsce-2017-analiza (access: 29.04.2018).

http://www.giodo.gov.pl/487/id_art/9146/j/pl/ (access: 26.04.2018).

https://avlab.pl/pl/ecm-insights-2017-tylko-25-europejskich-przedsiebiorstw-jest-gotowych-na-rodo (access: 26.04.2018 r.).

https://www2.deloitte.com/pl/pl/pages/press-releases/articles/wiekszosc-firm-wciaz-zwleka-z-wdrozeniem-RODO.html (dostęp: 29.04.2018).
https://www.computerworld.pl/news/Nie-ma-firmy-za-malej-na-bezpieczenstwo,409986.html (access: 26.04.2018).
https://www.computerworld.pl/news/Ponad-polowa-firm-nie-zaplanowala-jeszcze-budzetu-na-wdrozenie-RODO,409418.html (access: 29.04.2018).
https://www.itbusinessedge.com/articles/how-to-create-your-gdpr-budget.html (dostęp: 29.04.2018).
https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html (access: 28.04.2018).
https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (access: 26.04.2018).
https://www.statista.com/statistics/448431/perception-of-online-data-security-in-germany/ (access: 26.04.2018).