DOI: 10.20472/IAC.2018.041.013

ADAM FAIFR
Faculty of Economics, University of West Bohemia, Czech Republic

MARTIN JANUSKA
Faculty of Economics, University of West Bohemia, Czech Republic

COMPANIES´ READINESS OF GDPR AND IMPLEMENTATION BARRIERS

Abstract:

This paper deals with the topic of General Data Protection Regulation and its consequences for companies. Regulation defines new requirements that companies must meet by May 2018. These requirements changed the previous view on the management of personal data in organizations where some normative requirements became legally enforceable requirements. The circumstances of the adoption and requirements coming from new legislation are described as first while there is also outlined the relation with contemporal business administration approach and data protection management.
On this basis, the readiness of businesses is evaluated by triangulation of more available studies and the main factors influencing the preparedness are also identified and analyzed.
The final part is devoted to the process of GDPR implementation, consisting of carrying out the whole Data Protection Impact Assesment, as well as the mapping of data in organization.

Keywords:

GDPR, data protection, DPIA, information management, risk analysis, compliance

JEL Classification: G32, M15, D80

1. Introduction

At the end of May this year, a new EU regulation of the data protection of their citizens' personal data came into effect. The so-called GDPR brings several innovations that reinforce the rights of the citizens of the European Union in relation to the processing of their personal data.

Enhancing rights on the one hand also entails an increase of requirements to administrators and processors who will process these data. Over the last two years since the adoption of the regulation, several studies have been conducted to address the preparedness of businesses for forthcoming legislation. The latest results are known since April this year.

Although new regulations became effective in May, according to the available results, not all processors and companies are ready for change, thus they are now at a risk of violating personal data rights with a multiple of fines more than they used to be in the past.

The aim of this work is to examine and analyze the preparedness of companies in case of current legislation and to identify possible factors that prevent implementation.

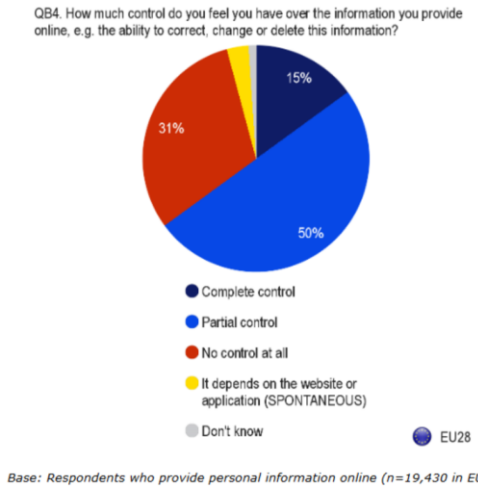
2. Demand for security

The GDPR Regulation, adopted by the European Union in April 2016, replaced the current legislation of the State members and previous EU regulations. It concerns all citizens of the European Union, all institutions and individuals processing personal data of citizens of the European Union. Personal data is considered as any information that can identify a particular individual, directly or indirectly. For such identifier can therefore be considered as one or a combination of different physical, physiological, genetic, psychological, cultural or social identities of the individual. An individual is referred to as the information subject in this Regulation (hereinafter GDPR). (Regulation (EU) 2016/679; The office for personal data protection, 2017)

The aim of the newly adopted regulation is to replace the existing European Union legislation adopted in 1995, which has become obsolete and has stop reflecting the data processing requirements in the context of technology development. The GDPR involves reinforcement of citizens' rights in relation to the processing of their data not only within the member state but also outside the European Union. Every resident should have an accurate view of how, and for what purpose are their personal data processed by administrators. Each Personal data manager should then be able to demonstrate how the data is being processed. (Regulation (EU) 2016/679; Mansfield-Devine, 2016)

What was the real reason for adoption of an updated regulation? With the development of the internet, there is an increase in internet purchases. This has consequences not only for the provision of personal data in order for the business to be carried out but also for their further use. One of these phenomena is, for example, the personalization of the internet, based on the data previously acquired, creating a custom-tailored ad for the user who is currently searching on the internet. If it is possible to collect sufficient data so that it can effectively address the advertisement, can it also be guaranteed that profiled data about it is used with its permission and can not be misused? (Special Eurobarometer 431, 2015)

Picture 1: Control over personal data



Source: Special Eurobarometer 431 (2015)

A partial answer can be found in the Eurobarometer survey, where two-thirds of Europeans says that they do not feel control over their online data, for example, when they use online payments or connect with friends through social networks. Symantec's findings are similar. What can be clearly seen in both surveys is that there is demand for increased protection. The processing of their personal data cause mistrust over time. The other fact is that they would like to have the same rights regardless of the country in which they wish to exercise their rights. (Special Eurobarometer, 2015; Symantec, 2015)

3. Contemporary data protection management

In terms of personal data management, two perspectives, both normative and legislative, can be distinguished. While the legislative sets out the legal framework for protection, the normative framework recommends a consecution leading to meeting all requirements. However, with the adoption of new legislation, this change is taking place.

3.1. Normative perspective

The first of personal data management perspectives is the normative one, which is a set of recommendations for the best results, also known as best practices.

In the field of information security, the generally accepted ISO 27 000 group of regulations governing the information security management system is in place. The Norm describes specific steps and practices leading to the protection of information assets, which is considered to be a cluster of information and data that has a value to the enterprise. (Gogela, 2015)

Information assets are further divided into primary and supporting assets. Primary assets are the information itself, whereas supportive assets are assets use for saving, processing and securing of primary assets. [1] (Škeřík, 2016)

The following table shows primary information assets in terms of their confidentiality.[2]

Table 1: Dividing of information from the point of view of its confidentiality

National organisation	**Private organizations**
Classified information	Unprotected informations
Personal data	Protected informations
Internal data	• Company internal informations
Other data	• Sensitive internal information
	Personal data

Source: own adjustment based on Škeřík (2016)

Personal data management according to ISO 27000

The procedure defined by the standard is fully based on the general risk management concept in the enterprise. In ISO 27000, the risk is considered as a possibility when the threat use the system's vulnerability and cause the damages of the asset. (Decree No. 316/2014)

[1] Some sources define three types of information assets – primary, supportive and technical assets.

The first step is to define the context of the organization according to the norm, ie to understand the goals of the organization, its activities and needs. The first step therefore determines the direction in which follow-up proceedings will be directed. The standard does not specify specific requisites, it only defines the internal and external aspects that should be taken into account when drawing up. (Škeřík, 2016)

The organization must further define the basic information security policy and also set employee responsibility for information security.

The next steps are identification of threats of all company assets and evaluation of its vulnerabilities. Subsequently, the variables are evaluated and the risk is adequately treated.

3.2. Legislative Perspective

The issue of the management of personal data is generally covered by the legislation of the individual member states. However, due to the adoption of a new legal directive, there are significant changes in this part where each country is obliged to develop new legislation that is in line with the GDPR regulation.

As already mentioned in the General Data Protection Regulation (abbreviated as GDPR), the new EU Directive defines a new legal framework for the protection of personal data of all citizens of the European Union. This replaces the previous directive of 1995.[3] The negotiation of the new directive began in 2012, when not only among the professional community was introduced under the designation GDPR. The new legislation was adopted in April 2016, with the effect of 25 May 2018. (Regulation (EU) 2016/679)

[3] Data protection directive

Relation with risk management:

Unlike the previous directive, the new regulation explicitly refers to risk. This is defined in two different perspectives:

- In terms of data leakage - the term risk is described as a risk of personal data leakage[4]
- In terms of potential sanctions - it describes the principle of fines in case of misconduct of organizations (Regulation (EU) 2016/679)

The second perspective describes the conenction between GDPR and risk management in companies, where on the one hand the impact of potential risk is quantified (the amount of the fine) conditioned by the probability that the central authority will grant the fine.[5]

The second of the proclaimed principles is an approach based on responsibility. This approach means that there should exist measures that minimize current risks.

As a consequence, the following obligations are newly defined:

- Implementation of data protection
- Data Protection Impact Assessment
- Appointment the Data Protection Officer
- Keeping records of personal data processing activities
- Necessity to consult before processing itself (Regulation (EU) 2016/679)

Data Protection Impact Assessment (DPIA) is one of the main steps in the implementation of the regulation into company where the potential risks to processing personal data are identified, evaluated and addressed. As stated in Microsoft's methodology, the following three basic steps are taken to process the document:

[4] For example, in the Preamble of the Regulation: „*Persons should be aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing*." (Regulation (EU) 2016/679)

[5] Enforcement of the Directive is entrusted to the so-called data protection authorities. For example, in the case of the Czech Republic, this is the Office for Personal Data Protection, which also decides on the amount of the fine imposed.

- Determination the range of DPIA
- Risk analysis
- Risk response (S.ICZ, 2017)

It follows from the above that the so far normative requirements concerning the management of personal data have been fully incorporated into the legislation. The ISO 27000 steps are no longer on the voluntary basis of each organization, but are imposed on each organization.

In table 2, the process of risk analysis (according to Microsoft methodology) is compared with the general risk management process as part of DPIA processing.

Table 2: Comparison of DPIA and risk management methodology

Model DPIA by Microsoft	**General risk analysis according to Smejkal**
Risk analysis • Risk acceptance criteria • Assets and their values • Threats and vulnerabilities • Risk assessment • Conformity analysis	**Risk analysis** • Determine of boundaries of risk analysis • Asset identification • Determination of value and grouping of assets • Threats identification • Threat and Vulnerability analysis • Phenomenon probability • Risk measurement

Source: own adjustment based on Microsoft (2017) and Smejkal (2013)

This implies that successful implementation of GDPR requirements also implies a advance in risk management (at least in the area of personal data) and within the organizations that have not been involved in the approach yet. Therefore, the assumption is that, as a result of the adoption of the GDPR, there will be a change in corporate risk management.

4. Methodology

This article analyzes the preparedness of companies operating in the European area in relation to the effectiveness of the GDPR Regulation. This analysis use the results of the studies that were presented between the adoption and the effectiveness of the Regulation, ie April 2016 to May 2018. During this period, a total of 6 studies were carried out, the main or secondary objective was to examine the readiness of companies at the time of their entry into force. These studies were also selected due to the internationalization of the survey, where not only businesses and representatives of companies from EU countries, but all concerned by the regulation, were addressed.

In terms of methodology, this is a data triangulation that aims is to monitor enterprise readiness from different perspectives. „*Triangulation can be used to combine different research methods*.“ (Denzin, p.786, 2007) Although triangulation does not increase or does not objectivizes the validity of the research, triangulation provides a more comprehensive view of the subject of the research. (Denzin, p.781, 2007). The use of this method is due to the absence of a sufficiently reliable research of the topic under consideration (as will be mentioned in the research section). The GDPR has, as mentioned, its impact on all organizations processing personal data of EU citizens, so it is necessary to combine the results of survey not only with European organizations.

Secondary data analysis is used in places where the same question is posed, and can be confirm or disprove the results with each other. In the following table, chronologically from left, are shown selected surveys with date when the survey was conducted, what was the main topic of the study, who were respondents and how many respondents participated in the study. All of these studies were processed online through a questionnaire survey.

Table 3: Survey overview

Published by:	**IaPP Truste**	**One Identity**	**Alert Logic**	**EY**	**Deloitte**	**ISACA**
Publishing date	November 2016	2017	July 2017	November 2017	January 2018	April 2018
Scope of survey	GDPR readiness and compliance techniques	GDPR readiness	GDPR Compliance	Data risk management	GDPR generally	GDPR readiness
Respondents	Companies in US, EU and Canada	Companies with European costumer base	EU companies	Companies using FDA	EMEA Countries	Members of ISACA
Number of respondents	244	821	200+	745	not specified	5045

Source: own adjustment based on studies reffered

The basic researches used in the work are iapp / Truste study presented shortly after the adoption of legislation, Alert Logic and ASACA study. All remaining studies due to their focus, complement the results of the studies. Usually, this was a partial or survey that primarily investigated another target.

In the case of the Iapp study, this is the first study that can be the following results compared with. At the same time, it is a study that identified barriers to implementation, not only on a general but also a specific level, when implementing partial deployment steps such as DPIA and data mapping. At work, the analysis is dedicated to these two steps.

5. Preparedness of organizations

The implementation of the GDPR principles, as mentioned, brings some new claims and a change of view to the processing itself. The whole process was outlined by the ICO (Information Commissioner's Office), which defines 12 main steps in preparation for the compliance. Steps that has to be taken by each administrator are based on safety standards ISO 27001 and ISO 27002. While ISO 27001 establishes organizational and technological measures to protect all information, ISO 27002 allows to determine the security of the organization's information system and also to

provide the starting point for its improvement. The implementation of the GDPR principles still brings some new requirements. (ICO, 2016; Tankard, 2016)

What does companies expect from the implementation of regulation principles? In this section, the results will be described, both in terms of the expected changes that regulation will bring, and expectations of self-preparedness as well.

The first common question is how big the expected impact on the company's internal business is. Answers can be found in selected surveys in One Identity and Alert Logic. The results show that a significant impact on risk management is expected by the significant majority of companies interviewed, where a significant impact expect between 23 % to 32 % of companies. (Alert Logic, 2017; One Identity, 2017)

Table 4: Impact on security practices

Survey	Alert Logic	One Identity
Substantial change	32 %	23 %
Minor or relatively minor change	61 %	66 %
No change	7 %	11 %

Source: own processing based on studies reffered

Another essential question is: „to what extent companies expect to be fully prepared at the time of the commencement of the regulation?“. Queries searching for this information can be found in the Alert Logic, Deloitte and ISACA studies. The first study was presented in the second half of last year, the remaining two were presented at the beginning of this year (January 2018 or April 2018).[6]

[6] The results are rounded to full percentage points.

Table 5: Preparedness of organizations

Survey	Alert Logic		Deloitte		ISACA	
Question	"How prepared is your company to meet EU GDPR regulations by the deadline of 25 May, 2018?"		"Compliance expectations by 25th May 2018"		"When do you expect your organization will be 100% GDPR compliant?"	
Answers:	**Already compliant**	5 %	**Fully compliant**	15 %	**By the 25 May 2018 deadline**	29 %
	Confindent of being compliant by deadline	28 %			**Q3/2018**	10 %
	Started with preparations, but not confident	27 %	**Opting for a risk-based, defensible position**	62 %	**Q4/2018**	13 %
					Q1/2019	7 %
	Not started yet	40 %	**Low expectation**	23 %	**Later than Q1/2019**	10 %
					Don´t know	31 %

Source: own adjustment based on studies reffered

Although each of the three surveys offers a different perspective in terms of readiness, the results are practically identical in that only a small part of data controllers will be ready in May 2018. Results from half of last year (Alert Logic) show that about a third is or will be fully prepared. The results of the last survey confirm the similar values (ASACA). So, most of companies are not ready for GDPR yet. (Alert Logic, 2017; ISACA, 2018)

The chronological view of three studies shows that 40 % of interviewed did not start preparations even in the middle of last year. The remaining 60 % began preparing with varying degree of certainty to be in time with deadline. At the same time, the proportion of those who are getting ready for regulation is still increasing. However, the Deloitte study from the turn of the year 2017 and 2018 reduces the borderline of those, who will be compliant, to 15 %. On the other hand, most of the respondents (62 %) are convinced that they will be largely prepared. The ISACA study then

complements the findings of the timing when the organization will be ready. [7] (Alert Logic, 2017; ISACA, 2018; Deloitte, 2018)

5.1. Identified barriers

In addition to the state of preparedness of companies, the possible causes of insufficient readiness at the time of the adoption of new legislation will be analyzed in this section.

Four of the selected studies were devoted into identification of barriers, or more precisely, challenges. Due to the differences in the methodologies of the individual studies, only the identification of the barriers that appeared across surveys was performed. Therefore, the identified barriers can not be ranked according to significance which is examined in individual studies.

The following table delimit repetitive barriers. These are further divided into external and internal. The most frequently mentioned external obstacle is the ambiguity of European legislation (2 times) and low priority on the part of management (3 times). The lack of time for implementation hampered to the fulfillment of the European regulation.[8] Due to the low priority of the companies, the other barriers were the low budget for implementation, the lack of qualified personnel, lack of available tools and technology in the companies. In the Deloitte study, respondents would expect greater support from central authorities. (iapp, 2016; Alert Logic, 2017; Deloitte, 2018, ISACA, 2018)

[7] 31 % of respondents to the ISACA study are not sure enough to meet the requirements in full. (ISACA, 2018)

[8] According to the ISACA study, 59 % of respondents should be ready by the end of the first quarter of the following year compared to the current 29 %.

Table 6: Identification of barriers

	iapp	Alert Logic	Deloitte	ISACA
Ambiquity of European legislation		X	X	X
Lack of time	X		X	
Lack of guidance by authorities			X	
Low priority	X	X		X
Low budget	X	X		
Lack of right tools or technology	X	X		
Lack of expert staff		X		

Source: Own adjustment based on studie reffered

5.1.1. The ambiquity of European legislation

In searching for barriers to non-fulfillment, among other things, one can find the difficulty of understanding clearly all the consequences of the regulation. This is one of the main problem that is mentioned in three of the four surveys. All this is in a situation where one of the target by the new legislation is the integration of the legal framework in the European Union. (Regulation (EU) 2016/679)

The issue here is not just the wording of the regulation itself, but also its enforcement. It is in entrusted to a central authority in each country that interprets and enforces individual articles. A comparison of 8 Member States was published in the article „A comparison of data protection legislation and policies across the EU“. In example 8 of selected European countries, was demonstrated that a existing regulation, which was to be enforced in a comparable way throughout the European area interpreted differently in each country. *„The actual protection, however, does not only depend on the legal framework, but also on the actual implementation and interpretation of the legislation and the ways in which it is enforced by courts and Data Protection Authorities (DPAs). The legislation on privacy and the protection of personal data contains many open norms that need further translation into workable, sector-specific, and context-specific rules and practices.“* (Custers et al., p.1, 2017)

From the perspective of entrepreneurs, this means that it is not possible to predict how far-fetched the consequences of the risk of default will be until it enters into force. This means that business entities, when assessing the benefits and costs of introducing GDPR elements into their own practice, will not be able to evaluate whether the steps leading to fulfillment are more economical than their non-compliance.

And whether they are sure to take the right steps at all. With the intent to explain Regulation more preciselythe European Commission has issued two corrections for some of the regulations before it enters into force.

5.1.2. Low priority

The most fundamental change, apart from the right to data portability, is the change in the amount of the maximum penalty that may be imposed. So far the highest fine given to commercial entity in the Czech Republic in connection with the processing of personal data was imposed to T-mobile for the release of more than 1.2 million customer data amounting to CZK 3.6 million (approximately EUR 140 thousand). It happened in a situation where the maximum fine could be granted in the amount of 10 million Czech crowns. There can be only guessed how much a fine would be imposed by the Office in the time of GDPR commencement, where the maximum fine could be around CZK 1 billion (EUR 39.5 million). (Škeřík, 2016)

Despite the risk, only about one third of the company will be fully prepared, studies say. Why then, companies, at least according to the latest data, has not better care? The answer can be found in the expectation of companies that, in only 33 % of cases, consider that the authorities will be interested only in biger companies. Considering that this is an analysis of secondary data, it is hard to conclude if it is the same part of firms that give the new regulation one of the highest priorities and are directing their activities to meet new obligations at the time of effectiveness. (Alert Logic, 2017)

The Alert Logic study provides a more detailed analysis. The results here also offer information in terms of company size, namely that the larger the company, the more important the issue is and give it a higher priority. There is also a clear connection with the fact that larger companies expected that implementing is both, time-consuming and costly task. At the same time, there is besides a risk of direct financial punishment also a risk of loss of credibility, which may also be reflected in their value. (Mansfield-Devine, 2016; Alert Logic, 2017; Ernst & Young, 2018)

The hypothesis also answers the question of the expected sanctions associated with the new legislation. 42 % of respondents believe that the fines imposed will be given rather as a warning, and they will forgive to most companies. About one-third of the people questioned are afraid of it and believe that a large number of companies will be affected. However, it can not be confirmed whether it is the same group that is convinced that it is or will be ready for GDPR. EY's findings then show that two-thirds

of respondents who are familiar with the GDPR principles are worried about sanctions by regulators. (Alert Logic, 2017)

Let's get back to the survey "A comparison of data protection legislation and policies across the EU". This survey follows up the budget-to-GDP link to data protection issues in the individual countries that has been analyzed. The countries ranged from less than 0.5 % of the annual budget, to 3 % dedicated to data protection each year. Although there was no relation between the size of the instrument dealing with this issue and the ability to evaluate individual suggestions has not been confirmed, the results are obvious. The importance of GDPR differs in particular countries and this disbalance will not bring the change in legislation either. When we compare the situation from point of view of risks, it can therefore be assumed that, while there is an advance in the possible impact (sanctions), then when there is unchanged levels of the central authorities' budgets, the total of the deeds in the countries concerned will remain at the same level as before. This won't increase the probability that the company will be affected. From the annual report of The Office for Personal Data Protection of 2016 it follows that they handled 1585 complaints in the year and carried out 116 own inspections. (Custers et al., 2017; The office for personal data protection, 2017)

5.2. DPIA

Let's see the whole process of deploying GDPR in the enterprise and identify factors that, in their own opinion, impede companies from an internal point of view in implementing.

Article 35 of the Regulation defines the processing of Data Protection Impact Assesment (DPIA), which is an impact assessment on the processing of personal data. The WP29 Working Group adds: *"DPIA is a key part of complying with the GDPR where high-risk data processing is involved."* In a nutshell, this is a report of analysis and risk management associated with the processing of personal data. (Regulation (EU) 2016/679; Guideline on DPIA, 2017)

DPIA process consists of three basic groups of steps. The first step is the description of the process of processing personal data, the second part is the risk analysis, the third is the measure identification. (S.ICZ, 2017)

Partial steps of DPIA are defined in the following table:

Table 7: Steps of DPIA

1. Scope of DPIA	**2. Risk Analysis**	
• Description of the assessed process of processing personal data	• Criteria for risk acceptance	
• Description of the evaluated information system or service	• Assets and their Values	**3. Measures identification** (consists only of this step)
• Description of operational procedures	• Threats and vulnerabilities	
• Description of interaction with the data subject	• Risk assessment	
• Privacy and Security Requirements	• Conformity analysis	

Source: own adjustment based on S.ICZ (2017)

How do the companies respond to assess DPIA? The intention to process the impact of assessment to the processing of personal data was reflected in 71 % of companies in 2016. Rather larger businesses had intention to process the Privacy. Unambiguous and even the main motivation for the processing of the Privacy Assesment is to compliance with the GDPR Regulation (80 % of the Member States, 54 % overall). In addition to this, other trigger can be found that companies do care about processing of personal data. Almost three quarters of all respondents, regardless of whether they are doing business in the EU or not, are processing or planning to process privacy assesment due to fulfilling its own internal regulations. Minority of the companies intend to process their privacy assesment because any of their business partner requires it (15 %). In this case, it is necessary to take a look if any company wants to do business in the European Union, they will have to observe with GDPR, otherwise it would incur the risk of fines. (iapp, 2016)

Although most businesses intend to process the privacy assessment, there are still about 25 % of companies that do not plan it. (iapp, 2016)

As it has been described earlier in this article, processing of privacy assesment consists of several steps. Most often, companies take approximately one working week to assess DPIA (21 %). One the other hand, 15 % of companies need more than one month to carry out the assesment, where the relation between company size and execution time can be observed. Usually because of wider involvement and deeper impacts. The time for processing, within the companies employing more than 5000

employees, the privacy assesment takes two working weeks in most cases. (iapp, 2016)

One of the first steps of DPIA, right after understanding the necessity of assesment conduction, is mapping of all personal data which are processed within the company. One of the biggest identified risk related to data processing is companies´ nescience in terms of which data are exactly processed. Not only: „What can not be measured, can not be managed as well.“ There is also no posibility to manage something you are not aware where you have it. For data to be effectively managed, it must first be sufficiently mapped and described. This statement is widely accepted in a businesses where 4 out of 5 companies consider data mapping as an important step towards meeting all required rules by mid-2018.

6. Conclusion

The results of the six studies used show that only a minority of companies are already fully prepared fot the new legal data processing framework. Only about one-fourth to one-third is fully prepared today.

The most important reasons identified for low readiness of GDPR are the ambiguity of adopted European legislation, particularly in terms of its interpretation and seemingly unclear enforcement by central authorities in the countries concerned.

Another important factor during the last two years was the low priority of the enterprises themselves. Organizations did not allocate sufficient resources, did not train their employees, did not take steps to fulfill the regulations. This can be partly due to the slackness of businesses that postponed the necessary steps, but also because of the ambiguities in legislation where it was not clear what needs to be done or which steps to take. In general, the lack of time seemed like another barrier.

A special part is given to compliance process itself, namely to conduction of DPIA. The available findings show that a significant majority of respondents have a plan to process the DPIA considering about one week to make it done. The results also show that time required for its processing is longer with the size of company.

Reference

An Overview of the General Data Protection Regulation (GDPR) (2017). Microsoft. Available at: http://download.microsoft.com/download/D/4/0/D40BB8BA-ED0A-4066-8EAF-FB07F279BD02/GDPR_Overview.pdf [Accessed 8 Apr. 2018].

Annual report 2016. The office for personal data protection in Czech republic. (2017). Available at: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=27256 [Accessed 8 Apr. 2018].

CUSTERS, B., DECHESNE, F., SEARS, A. M., TANI, T., & VAN DER HOF, S. (2017). A comparison of data protection legislation and policies across the EU. Computer Law & Security Review, 34(2), 234–243. https://doi.org/10.1016/j.clsr.2017.09.001

Decree No. 316/2014 Coll., On Security Measures, Cyber Security Incidents, Reactive Measures, and Cyber Security Submission Requirements (Cyber Security Regulation). In: THE COLLECTION OF LAWS. Prague: National Security Authority, 2014

EDITED BY NORMAN K. DENZIN. Sociological methods: a sourcebook. [Facsim. ed.]. New Brunswick, N.J: Aldine Transaction, 2007. ISBN 9780202308401.

General Data Protection Regulation (GDPR) Infographic. (2017) ONE IDENTITY. Available at:. https://www.oneidentity.com/infographic/general-data-protection-regulation-infographic8118615/. [Accessed 8 Jul. 2018].

GDPR Compliance in the EU. (2017) ALERT LOGIC. Available at: https://www.alertlogic.com/solutions/compliance/gdpr-compliance/

GDPR: The End of the beginning. (2018) ISACA. Available at: http://www.isaca.org/Knowledge-Center/Documents/2018-GDPR-Readiness-Survey-Report.pdf [Accessed 23 Jul. 2018].

GOGELA, R. Standards and definitions of information security concepts. In: CyberSecurity.cz: Kybernetická bezpečnost [online]. Available at: http://www.cybersecurity.cz/data/gogela.pdf [Accessed 23 Jul. 2018].

Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01). (2017) EUROPEAN COMISSION. Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 [Accessed 8 Apr. 2018].

How can you disrupt risk in an era of digital transformation? Global Forensic Data Analytics Survey 2018.(2018). ERNST & YOUNG. http://www.ey.com/Publication/vwLUAssets/ey-how-can-you-disrupt-risk-in-an-era-of-digital-transformation/$FILE/ey-how-can-you-disrupt-risk-in-an-era-of-digital-transformation.pdf [Accessed 18 Jun. 2018].

MANSFIELD-DEVINE, S. (2016). Data protection: prepare now or risk disaster. Computer Fraud & Security, 2016(12), 5–12. https://doi.org/10.1016/s1361-3723(16)30098-

Model DPIA and risk analysis for processing personal information in Microsoft Office 365. (2017) S.ICZ a.s. Available at: http://download.microsoft.com/documents/cs-cz/gdprsnidane/S.ICZ_MICR01817-Modelova_DPIA_Office_365-110_Final.pdf [Accessed 8 Apr. 2018].

Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now. (2016) INFORMATION COMMISSIONER´S OFFICE. Available at: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf [Accessed 21 Apr. 2018].

Preparing for the GDPR: DPOs, PIAs, and Data Mapping. IAPP. Available at:

https://iapp.org/media/pdf/resource_center/Preparing-for-GDPR_FINAL-1.0.pdf [Accessed 16 Jun. 2018].

Ready for GDPR. (2017) KPMG. Available at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/kpmg-gprd-guide.pdf [Accessed 1 Jul. 2018].

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016) EUROPEAN COUNCIL. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. [Accessed 8 Apr. 2018].

Special Eurobarometer 431: Data protection (2015) EUROPEAN COMMISSION. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf. [Accessed 15 Jun. 2018].

State of Privacy Report 2015. (2016) SYMANTEC. Available at: www.symantec.com/content/en/us/about/presskits/b-state-privacy-report-2015.pdf [Accessed 8 Apr. 2018].

TANKARD, C. (2016). What the GDPR means for businesses. Network Security, 2016(6), 5–8. https://doi.org/10.1016/s1353-4858(16)30056

The time is now The Deloitte General Data Protection Regulation Benchmarking Survey. (2018). DELOITTE. Available at:. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-nwe-gdpr-benchmarking-survey-november-2017.pdf [Accessed 8 Apr. 2018].

ŠKEŘÍK, O. Information security management system through the ČSN/EN ISO/IEC standard 27001. Hradec Králové, 2016. Diploma thesis. University of Hradec Kralove.