IBIMA Publishing
Journal of Information Assurance & Cyber security
https://ibimapublishing.com/articles/JIACS/2018/758054/
Vol. 2018 (2018), Article ID 758054, 9 pages, ISSN : 2165-9923
DOI: 10.5171/2018.758054

Research Article

The Impact of General Data Protection Regulation in The Accounting Profession – Evidences from Romania

Victoria Stanciu and Sînziana-Maria Rîndaşu

The Bucharest University of Economic Studies, Romania

Correspondence should be addressed to: Sinziana Rindasu; sinziana_rindasu@yahoo.com

Received date:21 March 2018; Accepted date:5 July 2018; Published date: 4 December 2018

Academic Editor: Cezar Toader

Abstract

The current level of technological development lead to an increased need of privacy and security regarding the personal data of individuals. To respond to the current needs, the new General Data Protection Regulation framework aims to provide the necessary guidance to avoid future data leakage of personal private date. It can be observed that some of the accounting processes need to be examined in order to ensure a full compliance with the requirements of the regulation. The main scope of this paper is to provide a glimpse in the current adoption and compliance with the GDPR regulation in the case of the accounting profession in Romania, as well as providing guidance for an easier compliance. To the best of the authors' knowledge, this is the first paper that investigates the correlations between the regulation and the accounting profession in the context of Romania, from an information security perspective. After conducting an empirical analysis to assess the current level of knowledge and compliance, the results highlighted that, at the time of the study, with less than 2 months before the adoption date at the EU level, there was a significant gap of knowledge and compliance in the case of the accounting profession in Romania. Still, it is expected for this gap to decrease in the future months once the deadline is approaching.

Keywords: General Data Protection Regulation, accounting, information security

Introduction

The constant evolution of the economic and digital environment brought an unquestionable variety of benefits, by increasing the quality of our activities and accelerating economic growth. The world as we are seeing it today relies on the technological progress: robotics, artificial intelligence and, as a result of generalized digitalization, on information security.

The technological progress changed during the last decades, leading to a huge amount of stored and shared data, as part of the value creation process. New developments

Cite this Article as: Victoria Stanciu and Sînziana-Maria Rîndaşu (2018), "The Impact of General Data Protection Regulation in The Accounting Profession – Evidences from Romania ", Journal of Information Assurance & Cyber security, Vol. 2018 (2018), Article ID 758054, DOI: 10.5171/2018.758054

that facilitated automation and enhanced the activities' quality started to be adopted as a new step toward the digital economy and technologies that store and handle data as a base for decision-making processes. However, the latest news on data breaches (originated from companies such as Yahoo, Uber and Deloitte) are clearly highlighting that sometimes we neglect to protect one of the most important competitive advantages: data privacy. Moreover, these incidents prove that all the companies, no matter their size, should be aware that they can experience, any time, a cyberattack.

As over the years, security reports presented an increasing trend on data leakage, which resulted in financial and reputational losses, personal data and sensitive data exposure. As per this, in order to protect companies and individuals at the same time, a clear and efficient framework should be implemented.

At the European Union level, until now, there has been a regulation adopted in 1995 regarding personal data security. However, during the years, things have dramatically changed along with the need for a better privacy agenda. In order to cope with the existing technologies and provide a sufficient level of protection, a new regulation will come in place, starting May 2018. This General Data Protection Regulation (GDPR) is extending the previous rules, by enhancing the need for awareness of personal data breaches, compliance and accountability. Over the last couple of years, this regulation continues to create restlessness to the majority of companies worldwide, as it affects core processes and the noncompliance consequences cannot be ignored.

Since 2016, when the regulation has been made public, researchers from different domains started to assess how the GDPR will impact different activities, such as marketing and IT. However, little information has been provided on the impact of the regulation in regards to the accounting processes, which are using a significant amount of personal data.

This paper is focusing on the processes that include the use of personal data by the accounting departments, such as employees, customers, consultants and third party information, along with the effects that the new regulation brings in order to increase the security of this kind of data. Due to their nature, the accounting processes use a significant amount of personal data. As per this, we consider it important to analyze how the information storing and manipulation have to be done in order to comply with the regulation.

The main objective of the study is to assess the impact of the General Data Protection Regulation in the case of accounting departments, along with the solutions accountants can use to meet the terms. As there is not much left until all companies that process EU citizens' data have to be on the right track, we considered it appropriate to investigate the current level of compliance and the awareness of accountants in Romania.

Literature Review

The General Data Protection Regulation, as previously mentioned, cannot be considered a new step in data protection (Mittal, 2017), as the actual purpose of this current framework is to balance the actual digital economy and personal privacy. The impact of breaches regarding personal data cannot be overlooked. As we can see from the recent data exposure affecting Equifax, the personal data of more than 145 million US citizens has been compromised, due to open-source vulnerabilities, for which the patch has not been applied in due time, giving the attackers a chance to stole personal data (Hedley and Matthew, 2017). The total costs of this incident have not been made public, as the company expects to incur other costs in the near future for this event. This case can be seen as an example that clearly shows the financial and reputational impact of data security breaches.

Despite the fact that the GDPR regulation has been made public in 2016, the majority of companies are still concerned with the possible implications it can bring, as prior

Victoria Stanciu and Sînziana-Maria Rîndaşu (2018), Journal of Information Assurance & Cybersecurity,
DOI: 10.5171/2018.758054

researchers emphasized (Ford and Qamar, 2017; Seo et al., 2017), due to the fact that on short-term the business models and strategy can be disrupted.

GDPR divides the privacy owners into two categories: the controller, who should be in charge of the purpose and means of processing personal data and the data processor, who should process the data on behalf of the controller. Each actor is responsible for the personal data managed in compliance with the regulation. However, giving the fact that this regulation has not been yet applied and the framework is considered not clear enough to cover all the possible scenarios and provides little insight, especially when it comes to technical matters such as security controls (Lindqvist, 2017; Wachter et al., 2017; Mansfield-Devine, 2017), there is a general concern that this regulation will bring more disadvantages – especially cost related, than benefits, on short-term. However, there can be also benefits on the long-term, as for example the principles stated by the regulation which will help the companies to build a solid framework regarding personal data privacy and decrease the risk of data breaches, if the security measures are properly implemented (Beckett, 2017). Another benefit brought by GDPR, as Zerlang (2017) states, is that the guidelines of this regulation increase the speed of data normalization processes, along with creating a context to identify in a more timely manner the possible anomalies.

The accountability principle is part of the new main changes which requests the controllers to take all the appropriate measures to comply with the regulation and in the same time to be able to prove that the company has performed its activities in line with the compliance rules. Yet, the framework is not providing clear rules on how to demonstrate accountability, which can be considered another drawback of the regulation. However, professional bodies such as the Institute of Chartered Accountants in England and Wales (2018) started to provide support to the practitioners to comply with the GDPR, highlighting the fact that accountability can be proven by having implemented the best practices related to data privacy, along with cybersecurity regulations and standards.

Another new part of the regulation is the introduction of the "right to be forgotten", which refers to the fact that the personal data stored by companies should be deleted from their database, along with any records shared with third parties, if the individual makes such request. This aspect increases the natural persons' power to control how their personal data is handled (Sobolewski et al., 2017) and enhances, at the same time, the level of transparency. However, this rule does not apply in cases in which other laws clearly express that the data should be stored for a certain period of time. Nonetheless, even though this new idea seems to be straightforward, the practical implementation of it can generate, on short-term, series of costs and on the technical side this outcome can be quite difficult to achieve (Villaronga et al., 2017).

The Impact Of The General Data Protection Regulation On The Accounting Processes

The accounting processes are complex and involve a significant amount of information collected from several departments of the organizations and in the majority of the cases, the accountants have to deal with personal data, such as employee data – for the salaries and social contributions records, new and existing clients' data – if the clients are natural persons, consultants or any other third parties. In respect to this aspect, if the personal data the accounts use refers to an EU individual, their processing and handling activity should be complying with GDPR. Even though the main goal of the directive is not to penalize organizations, but to help them to achieve a better degree of control over personal data processing, the risk of not being able to follow the rules can result in fines up to 4% of the turnover, which is not an option for the majority of corporations.

It can be difficult for accountants to apply and advise the best practices to be in compliance with the GDPR in the absence of a good understanding of the main

information security measures to prevent data breaches. As per this, training the accountants to handle and prevent data leakages should be the first step in starting the GDPR adoption. The Verizon 2017 Data Breach Investigations Report highlights the fact that attackers usually target HR or accounting employees in an organization, as they are more likely to open links and attachments. This output seems to be quite concerning as these departments are the ones which manage significant amounts of personal data. Moreover, the same report presents that in 81% of the cases, the attackers are taking advantage of weak and stolen credentials.

Unless the accountants increase their level of awareness and their capabilities of being able to protect any kind of sensitive or personal data, there is a high risk that the compliance with GDPR will not be fully achieved. As per this, we believe that a solid base of knowledge regarding data protection and attacks methods is the first step for accountants to be able to meet the terms of the regulation.

Seeing the big picture with the GDPR's rules and principles, this can seem to be quite clear, but when actually trying to raise the level of awareness of the accountants and create a control framework for them to comply with the new rules, it can be a bit unclear, due to the massive segregation of processes in organizations. The international accounting professional bodies have already started to create a set of practical guidelines (ICAEW, 2018; ACCA, 2017), to help the professionals adapt easier and understand how they can play a vital role in maintaining the privacy of personal data. Moreover, ACCA (2017) highlights the fact that accountants should be able to provide support in lawfully using personal data.

Even though the international professional bodies are trying to provide guidelines for accountants, these recommendations are based rather on principles than on clear rules and action plans. In accordance, the GDPR adoption will be quite challenging for the accounting professionals, at least in the first months, as they will have to create a complete framework of the data stored and manipulated, along with the purposes of using that information.

As it has been previously presented, in the recent years, many researchers started to assess the impact of the regulation in respect of the IT activities and controls, but less attention has been paid to the changes that the GDPR can bring in the accounting information processing. In this part of the paper, we are trying to identify the main accounting activities that use personal data and how these processes can, from the accountants' perspective, follow the requirements of the regulation. Nevertheless, we must keep in mind the fact that the accountants have limited abilities to use and understand complex IT security solutions and, due to this, their competences can cover only the non-technical part of the data privacy.

The main activities that would require, in the authors' opinion, an increased level of protection, not only for the GDPR compliance but also that can be applied in order to secure any kind of confidential, sensitive or personal data are:

- Physical security of the mobile devices and physical supporting documentation on personal data –strict policies that dictate how the employees should store sensitive or personal data should be issued, along with the use of credentials of accessing that kind of information;
- Strong passwords and best practices of keeping the credentials secured – the employees, as well as the companies, should take all the appropriate measures to decrease the risk of stolen credentials and attacks due to weak passwords;
- Not sending confidential or personal data unless this is absolutely necessary, a case in which the information should be password protected, such as secured spreadsheets and documents;
- Constantly reviewing the databases in which the personal and confidential information is set, in order to flag any kind of obsolete data or anomalies;
- Maintaining and timely updating any kind of backup documentation and consent of processing personal and confidential data;

- Addressing any possible data leakage concerning the Data Protection Officer in a timely manner;
- Creating and maintaining up to data the master data records and mapping the information in accordance with a specific purpose of using those data;
- Identifying all the accounting flows that produce or manipulate personal data and suggesting appropriate measures to secure those specific work flows;
- Reviewing all the policies for processes that use personal and confidential data to check the compliance of the policies with the GDPR regulation.

As it can be easily observed, the majority of the above-presented measures aiming to decrease the data leakages are not only meant for the accounting departments, but these can be implemented by any other department that stores or process personal data.

The GDPR is still considered to create some uncertainties among organizations as the existing framework seems not to cover all the possible scenarios. In this regard, we consider that in the near future, it is expected to identify more issues to emerge in respect of trying to meet the regulation.

Research Methodology

After analyzing the potential impact that GDPR might have on the accounting activities, we considered it appropriate to assess the accountants' and auditors' level of awareness in regard to this new regulation. As per this, we have conducted a study, based on a survey. The questionnaire was sent to 200 accountants, financial and internal auditors working in Romanian companies and the responses were collected between the 1st and 15th of March, with a bit more than 2 months before the GDPR enforcement.
The aim of this survey was to find out if the accounting and audit professionals are aware of this regulation and whether they have started to review their activities in order to comply with it.

The questionnaire was designed to cover all the GDPR topics, from the accounting activities' perspective and comprised of 11 close-ended and semi-close-ended questions that focused on the understanding of the respondents. The participants had also the possibility to choose from several options. We tried to limit the number of questions in order to avoid any kind of redundant or known answers.

When sending the survey, we took into account the fact that multiple answers from professionals working in the same company will affect the accuracy of the research. As per this, when sending the invitation to participate at the survey, we tried not to send it to more than 2 persons employed by the same company. The questionnaire was sent using professional networks, such as LinkedIn and we used other professional communities to select our possible respondents. As we considered it appropriate to maintain a certain level of confidentiality, the participants have not been asked to name the companies they are working for.

During the two weeks in which the participants completed the questionnaire, we collected 109 answers, having a response rate of 54.5% and no forms have been excluded, as all of the received forms were complete and matched the requirements set for this study.

The professional experience of the respondents varies from 1 to more than 5 years of experience and the structure is balanced as the majority of the respondents 36.7%, has between 2 and 5 years of experience, while 33% of them have more than 5 years of practical experience and the rest of 30.3% between one and 2 years. Moreover, the participants are working for companies of different sizes, depending on the number of employees, such as small companies, which represented the majority, medium size and large companies. The distribution of the respondents reported to the companies size can be observed in the below figure.

Fig 1: Respondents' distribution based on the company size

Source: own processing of the authors, based on the collected data

Data Analysis and Research Findings

From the responses received, we found that 51.37% of the respondents are members of professional certified national and international accounting and audit associations. As it has been highlighted in the previous section of this paper, the professional organizations have started to provide a base for a better understanding of the impact and possible ways of action during the GDPR enforcement, for all the individuals inside or outside the organizations.

The participants have also been asked if they are working with any kind of personal data such as full names, social security numbers, bank account numbers or any other information that might lead to the identification of the individuals, as per the definition given in the GDPR framework. After analyzing the responses, the fact that more than 83% of the respondents are working and storing such information has been highlighted.

Another question of the questionnaire was if the participants know anything about this regulation and the results showed that only 61.5% are familiar with it. The difference is quite significant as we conducted a more in-depth analysis, which emphasized that from that 83 % of persons who are dealing with personal data, 35% of them did not know anything about GDPR until the moment they participated in the study, while 44% of the respondents, who stated they do not use personal data confirmed their knowledge about the regulation. Nevertheless, we must keep in mind the fact that this study was conducted 2 months before the GDPR would be applied in Romania, andin all the other EU countries as well, so we expect that this knowledge gap will decrease in the next couple of months.

Due to the fact that we are focusing mainly on the potential impact of GDPR and we are trying to assess the level of knowledge of the practitioners, starting from this point, we will focus the analysis only on the respondents who advised that they are indeed using personal data.

When asked if the companies they are working for informed them about the regulation, more than 35.15% of the participants answered affirmative and 24.17% expect that they will be soon informed, while 40.65% of the participants do not know if they will be informed or not. Analyzing this aspect in-depth, we found out that from that 40.65 % of respondents, 35.17% are working in companies with more than 250 employees, while the majority is represented by employees working in small and medium companies. Giving the fact that the majority of the respondents stated that their companies did not inform them yet about GDPR, we consider this as being a bit alarming,

especially due to the fact that it might take some time until the organizations prepare a clear framework and the personal data processing activities are identified and compliant. Nonetheless, again we expect that these discrepancies will decrease in the near future.

The following two questions of the survey focused on the main activities performed by the practitioners, that require the use of personal data. Asked if they managed to identify, so far, which are the activities that fall into the GDPR regulation, just 52.74% stated that they already started to identify and classify those activities, while the rest of 47.26% have not. Moreover, the questionnaire also inquired if the professionals reviewed their work procedures on those activities and the result emphasized that only 37.36% of the participants responded affirmatively. We can notice that along the way, in our research, the knowledge gap kept on extending, emphasizing a concerning low level of awareness and action plans. Nonetheless, these results can also be explained through the company size, as, after reviewing these results in contrast with the company size, we found out that the majority of respondents who stated that the procedures have not been revised are working in companies with less than 250 employees, where the impact of GDPR might not be so intense, if their main activities are not based on personal data processing.

More details regarding the structure of the responses correlated with the size of the companies can be seen in the below table.

Table 1: The distribution of responses based on the size of the companies

	Identification of activities that use personal data		Reviewing the policies of the activities that use personal data	
Number of employees	Yes	No	Yes	No
Less than 100	22	21	14	29
Between 100 and 250	12	7	6	13
More than 250	14	15	14	15
Total	48	43	34	57

Source: own processing of the authors, based on the collected data

As it can be observed from the above table, there is a gap between the identification of activities and the actual revision of the work procedures, in the case of small and medium companies, while in the case of large companies the trend is stable. Nevertheless, the result can be justified by the fact that usually, large companies have a complete track of the activities and procedures and a better level of segregation, compared with the other types of companies.

So far, after reviewing the results of the survey, we can conclude that in Romania, there is clearly a knowledge gap in regard of the GDPR implementation, as the professionals are not properly informed and their activities are not fully reviewed in order to comply with the regulation. However, we must keep in mind the fact that there are still some months left until the compliance deadline and a decrease of the gap there is, therefore, expected.

As we have also presented in the previous section of the paper regarding the proper ways in which accountants can comply with GDPR, we have asked the participants to respond to a question regarding the security measures they are taken, in order to keep their data secured. The results can be seen in the figure 2.

As it can be observed from the chart, the main method used by the respondents is changing the password on regular basis, this is usually a requirement of the majority of the systems used nowadays.

However, the second choice of the participants is showing that they are indeed starting to improve the security of their accounts, even due to password combination restrictions or not, this is a favorable aspect. The third option should raise a flag, in the light of recent ransomware incidents. Nonetheless, this result is enforcing the Verizon result, concluding that the accountants can be considered extremely vulnerable. Securing the attachments when sending by email is a good practice in order to avoid any man-in-the-middle attack, however, as it can be noticed from the chart, this technique is used by extremely few professionals.

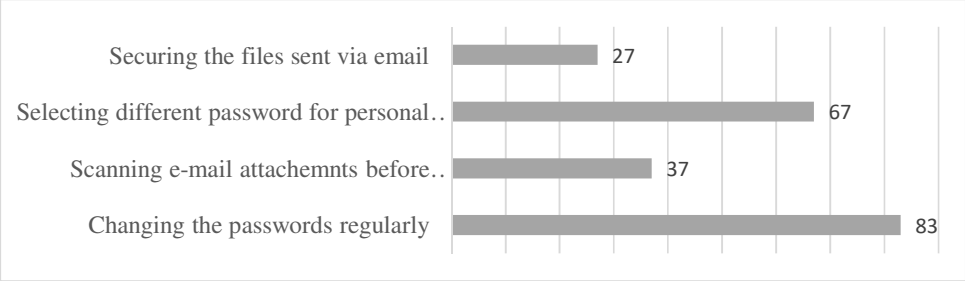

Fig. 2: Means to secure the activities

Source: own processing of the authors, based on the collected data

Even though the participants had the possibility of adding any other protection methods besides the above four means presented, no other answer has been received, despite the fact that the list we provided is not entirely complete. This creates the impression that they do not have yet a full understanding of the security measures and the possible impact of security breaches.

Conclusions

After analyzing the potential impact that the GDPR regulation can have on the accounting activities, we managed to highlight the main areas in which there might be changes in the main accounting activities based on personal data processing. As it has been presented, the professional bodies are making efforts in providing the practitioners a sufficient support in order to comply with the regulation. However, without the support of the companies, for which the practitioners are working, and a smooth collaboration with the IT departments, the compliance will not be possible, as a full and complete compliance needs an efficient collaboration between all the departments involved in the data processing accounting and HR activities.

After conducting the empirical research of assessing the level of awareness among Romanian accountants and auditors in respect of the GDPR, the results clearly highlighted a knowledge gap between the actual practice and the expectations. However, there is still enough room and time for improvement, until the deadline on 25th of May 2018. Moreover, after analyzing the practices of the accountants in order to secure their activities, the fact that they might not be fully understanding the means of protecting personal and private information has been highlighted, as their behavior is yet to be improved.

As this study was conducted with a couple of months before the GDPR enforcement, the authors expect a decrease of the knowledge gap to be discovered, in the near future, more closely to the regulation enforcement deadline. Nonetheless, we also expect an overall enhancement of the security practices in the accounting departments after GDPR, but not only limited to personal data processing.

Acknowledgment

The paper was presented in the 31st International Business Information Management Association (IBIMA) conference 2018 and the authors benefited of the recommendations of the editorial board. The present paper integrates the recommendations and feedback received.

References

1. Beckett, P. (2017). 'GDPR compliance: your tech department's next big opportunity', *Computer Fraud & Security*, (5), 9-13.
2. Ford, D. T., and Sreman Q. (2017), 'Seeking opportunities in the Internet of Things (IoT):: A Study of IT values co-creation in the IoT ecosystem while considering the potential impacts of the EU General Data Protection Regulations (GDPR)', [Online], [Retrieved March 18, 2018], http://umu.diva-portal.org/smash/record.jsf?pid=diva2%3A1117005&dswid=-1907
3. Hedley, D., and Matthew J.. 'The shape of things to come: the Equifax breach, the GDPR and open-source security', *Computer Fraud & Security*, 11, 5-7
4. Institute of Chartered Accountants in England and Wales (2018), "GDPR for Accountants: Your Questions Answered", [Online], [Retrieved February 28, 2018] https://www.icaew.com/-/media/ corporate/files/technical/information-technology/cyber-resource-centre/faqs-what-does-gdpr-mean-for-accountants
5. Lindqvist, J. (2017), 'New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? ', *International Journal of Law and Information Technology*, 1-19
6. Mansfield-Devine, S. (2017), 'Meeting the needs of GDPR with encryption', *Computer Fraud & Security*,(9), 16-20.
7. Mittal, I. P. S. (2017), 'Old Wine with a New Label: Rights of Data Subjects Under GDPR', *International Journal of Advanced Research in Computer Science*, 8: 67-71
8. Regulation, General Data Protection. "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." Official Journal of the European Union (OJ) 59 (2016): 1-88.
9. Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2017), 'An analysis of economic impact on IoT under GDPR', Information and Communication Technology Convergence (ICTC), , ISBN 978-1-5090-4032-2, 18 October 2018, 879-881
10. Sobolewski, M., Mazur, J., & Paliński, M. (2017), 'GDPR: A Step Towards a User-centric Internet? ', *Intereconomics*, 52(4), 207-213.
11. The Association of Chartered Certified Accountants (2017) "Ethics and trust in a digital age", [Online], [Retrived at February 28, 2018] http://www.accaglobal.com/content/dam/ACCA_Global/ Tech nical/Future/pi-ethics-trust-digital-age.pdf
12. Verizon (2017), "2017 Data Breach Investigations Report", [Online] [Retrived February 28, 2018] https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf
13. Villaronga, E. F., Kieseberg, P., & Li, T. (2017), 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten', *Computer Law & Security Review*
14. Wachter S., Mittelstadt B. and Russell C., (2017), "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR", Working paper, [Online], [Retrived March 1, 2018] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289
15. Zerlang, J. (2017), 'GDPR: a milestone in convergence for cyber-security and compliance', *Network Security*, (6), 8-11