International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278–9960; ISSN(E): 2278–9979
Vol. 10, Issue 1, Jan–Jun 2021; 65–74

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

EVIDENCE FROM INDIA: THE EFFECT OF THE GENERAL DATA SECURITY LAW ON THE ACCOUNTING PROFESSION

Y. Bhaskar Reddy[1], Shaik Khajakhizar[2] & B. Sudarshan[3]

[1,2]Assistant Professor Department of Computer Science Engineering, K.S.R.M College of Engineering, kadapa-AndhraPradesh-India-516003

[3]Associate Professor, Department of Mechanical Engineering, K.S.R.M College of Engineering, Kadapa, AndhraPradesh-India-516003

ABSTRACT

The present degree of technological advancement is contributing to an increased need for privacy and protection in relation to individuals' personal data. In order to respond to current needs, the new structure of the General Data Protection Regulation aims to provide the required guidelines to prevent the potential leakage of personal private data. In the case of the accounting profession in Romania, the key scope of this paper is to provide an overview of the current implementation and enforcement of the GDPR regulation, as well as to provide guidelines for easier compliance. To the best of the knowledge of the writer, this is the first paper that explores the relationships between the regulatory and accounting profession in the sense of Following an empirical review to determine the current level of knowledge and compliance, the findings highlighted that there was a major knowledge and compliance deficit in the case of the accounting profession in Romania at the time of the report, less than 2 months before the date of acceptance at EU level. Nevertheless, this difference is predicted to decrease once again in the coming months.

KEYWORDS: *Policy on General Data Protection, Accounting, Information Security*

Article History

Received: *11 Apr 2021* **|** ***Revised:*** *19 Apr 2021* **|** ***Accepted:*** *28 Apr 2021*

INTRODUCTION

By raising the efficiency of our operations and stimulating economic development, the relentless transformation of the economic and digital world has brought an unquestionable variety of benefits. The world we see today depends on technological progress: automation, artificial intelligence, and information security as a result of generalized digitalization.

As part of the value creation process, technological progress has changed over the last few decades, leading to a huge amount of stored and shared data. As a new step towards the digital economy and technologies that store and handle data as a basis for decision-making processes, new developments that facilitated automation and enhanced the quality of the activities began to be adopted. Nevertheless, the latest data breach news (from businesses such as Yahoo, Uber and Deloitte) clearly shows that we often struggle to secure one of the most significant competitive advantages: data privacy. In addition, these events show that all enterprises, no matter their size, are vulnerable. They should be mindful that they can encounter a cyber attack at any moment.

Security studies have shown a rising trend towards data leakage over the years, resulting in financial and reputational damages, personal data and exposure to sensitive data. As a result, a transparent and effective system should be introduced in order to protect businesses and individuals at the same time.

Until now, there has been a regulation at European Union level introduced in 1995 on the protection of personal data. However, along with the need for a stronger privacy agenda, things have changed drastically over the years. A new regulation will be in force beginning in May 2018 to cope with existing technology and provide an appropriate degree of security. This General Data Protection Regulation (GDPR) expands the previous rules by increasing the need for awareness, enforcement and accountability of personal data violations. This legislation has continued to generate anxiety for the majority of enterprises around the world over the last few years, as it affects key processes and the effects of non-compliance cannot be overlooked.

Researchers from various fields have begun to analyze how the GDPR could affect various practices, such as marketing and IT, since 2016, when the legislation was made public. Few information has, however, been presented on the effect of the Legislation on accounting processes using a large amount of personal data.

This paper focuses on the processes concerning the use of personal data by accounting departments, such as information from staff, clients, contractors and third parties, as well as the influence that the current legislation has on the security of this type of data. The accounting systems use a large amount of personal data because of their existence. As per this, in order to comply with the regulation, we consider it necessary to examine how data storage and manipulation must be done.

The main objective of the analysis is to determine the effect of the General Data Protection Legislation, along with the solution account, in the case of accounting departments.

After the legislation was made public in 2016, scholars from various fields have begun to analyze how the GDPR could influence various practices, such as marketing and IT. However, little information has been given on the effect of the legislation on accounting systems using a large amount of personal data.

This paper focuses on the processes concerning the use of personal data by accounting departments, such as information from staff, clients, contractors and third parties, as well as the influence that the current legislation has on the security of this type of data. Accounting systems, by their very nature, involve a large amount of personal data. As per this, in order to comply with the regulation, we consider it necessary to examine how data storage and manipulation must be done.

The main objective of the analysis is to analyze the effect of the General Data Protection Regulation on accounting departments, along with the solutions that accountants can use to satisfy the demands. Since there isn't much time until all companies that process EU citizens' data must be compliant, we figured it would be useful to look into the current level of compliance and accountant knowledge in India.

LITERATURE REVIEW

As previously noted, the General Data Protection Regulation (GDPR) cannot be considered a new phase in data protection (Mittal, 2017), because the existing framework's primary aim is to strike a balance between the digital economy and personal privacy. Personal data breaches have far-reaching implications that must not be ignored. As we can see from the

recent Equifax data breach, the personal data of over 145 million US people was exposed due to open-source vulnerabilities for which the fix was not implemented in a timely manner, enabling attackers to steal personal data (Hedley and Matthew, 2017). The cumulative cost of this incident has not been revealed because the company expects to incur further expenses in the near future as a result of this incident. This case can be used to explain the financial and reputational implications of data security breaches.

Despite the fact that the GDPR legislation was made public in 2016, the majority of businesses are still worried about the potential effects, as previous research has shown (Ford and Qamar, 2017; Seo et al., 2017), since business models and plans can be disrupted in the short term.

The data 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, are the two types of privacy owners identified by GDPR. Each actor is accountable for the personal data they handle in accordance with the law. However, given that this regulation has yet to be enforced and that the structure is deemed inadequate to cover all potential scenarios and provide little insight, especially in technical matters such as security controls (Lindquist, 2017; Watcher et al., 2017; Mansfield-Devine, 2017), there is widespread concern that this regulation could result in increased costs. However, there could be long-term benefits, such as the guidelines outlined in the legislation, which will assist businesses in creating a solid foundation for personal data protection and reducing the possibility of data breaches if security measures are properly enforced (Beckett, 2017). According to Zealand (2017), another advantage of GDPR is that its guidelines improve the speed of data normalization processes while also providing a framework for detecting potential anomalies in a timelier manner.

The accountability concept is one of the big improvements, and it allows controllers to take all required action to comply with the legislation while still showing that the company followed the rules. However, the framework does not have specific instructions for demonstrating transparency, which is another weakness in the statute. Professional bodies, such as the Institute of Chartered Accountants in England and Wales (2018), have begun to assist professionals in compliance with the GDPR, stressing that transparency can be demonstrated by using best practices data privacy regulations and standards, as well as cyber security regulations and standards

Another new provision of the legislation is the implementation of the "right to be forgotten," which specifies that if an entity requests it, personal data retained by corporations, as well as any information exchanged with third parties, should be removed from their databases. This function strengthens natural persons' ability to monitor how their personal data is managed while also the accountability (Sobolewski et al., 2017). This rule does not apply, however, in situations where other laws specifically specify that data must be held for a particular amount of time. Nonetheless, although this new definition seems clear, its practical implementation will result in a series of costs in the short term, as well as a technological outcome that is difficult to achieve (Villaronga et al., 2017).

THE GENERAL DATA PROTECTION REGULATION'S EFFECT ON ACCOUNTING PROCESSES

Accounting procedures are complicated and require a large amount of data obtained from many divisions of organizations, and in the majority of cases, accountants must deal with personal data, such as employee data – for salaries and social contribution records, new and existing client data – whether the clients are natural persons, consultants, or some other third party – and in the majority of cases, accountants must deal with personal data, such as employee data – for salaries and

social contribution records, new and existing client data – whether the clients are natural persons In this regard, if the accounts' personal data pertains to an EU entity, their processing and handling activities should be GDPR compliant. Despite the fact that the directive's primary purpose is to assist companies in achieving a greater level of control over personal data processing, failure to comply with the regulations will result in penalties of up to 4% of annual sales, which is out of reach for the vast majority of businesses.

In the absence of a good understanding of the key information protection measures to avoid data breaches, accountants can find it difficult to apply and advise the best practices to be in accordance with the GDPR. As a result, the first step in implementing GDPR should be to train accountants on how to manage and avoid data leaks. According to the Verizon 2017 Data Breach Investigations Report, attackers normally target HR or accounting workers in a business because they are more likely to open links and attachments. This performance tends to be very disturbing, considering that these departments are in possession of vast volumes of personal information. Furthermore, according to the same study, attackers misuse poor or stolen credentials in 81 percent of cases.

There is a high risk that GDPR compliance will not be completely achieved unless accountants improve their level of knowledge and skills in protecting some form of confidential or personal data. As a result, we agree that for accountants to be able to follow the terms of the legislation, they must have a strong foundation of expertise in data protection and attack methods.

When looking at the big picture of the GDPR's rules and principles, it can seem to be very straightforward, but when it comes to actually raising accountants' consciousness and establishing a management system for them to comply with the new rules, it can be a little hazy, due to the vast segregation of processes in organizations. International accounting professional bodies have also begun to establish a set of realistic guidelines (ICAEW, 2018; ACCA, 2017) to assist accountants in making the requisite changes and recognizing how they can play a critical role in protecting personal data privacy.

Despite the fact that international professional associations are attempting to include accounting guidance, these recommendations are based on principles rather than specific rules and action plans. As a result, the GDPR adoption will be difficult for accountants, at least in the beginning, since they will need to establish a detailed framework of data stored and manipulated, as well as the purposes for which that data will be used.

As previously stated, several researchers have begun to assess the effect of the regulation on IT activities and controls in recent years, but less attention has been paid to the changes that the GDPR may bring to accounting data processing. We are attempting to describe the key accounting practices that use personal data in this section of the paper, as well as how these procedures can be made to comply with the regulation from the accountant's perspective. However, we must bear in mind that accountants' abilities to use and comprehend complex IT protection solutions are restricted, and as a result, their competences are limited.

The following are the key activities that, in the authors' view, will necessitate a higher level of security, not only for GDPR enforcement but also to safeguard any kind of confidential, sensitive, or personal data:

Physical protection of mobile devices and supporting documents on personal data – specific rules dictating how workers can store confidential or personal data, as well as the use of passwords to access that information, should be provided.

Good passwords and best practices for keeping credentials safe – workers and businesses should take the required steps to reduce the possibility of credentials being stolen credentials and attacks caused by passwords that are too easy to guess.

Sending sensitive or personal data only when absolutely appropriate, in which case the data should be password protected, such as encrypted spreadsheets and documents;

Constantly checking the databases where personal and sensitive information is held in order to find any outdated information or anomalies;

Maintaining and regularly reviewing any backup documentation, as well as giving consent to the processing of personal and confidential information;

Responding immediately to any apparent data breach involving the Data Protection Officer;

Creating and preserving up-to-date master data records, as well as mapping information according to a particular reason for using such data;

Identifying all accounting processes that generate or exploit personal data and recommending effective security measures for those processes;

Examining all procedures for systems that use personal or sensitive data to ensure that they are GDPR compliant.

As can be seen, the majority of the above-mentioned data-leakage-prevention steps are applicable to every department that stores or processes personal data, not only accounting departments.

The GDPR is still seen as a source of uncertainty among businesses, as the current system seems to fall short of covering all possible scenarios. In this regard, we believe that further problems will arise in the near future as a result of attempting to comply with the regulations.

METHODOLOGY OF RESEARCH

Following our analysis of the possible effect of GDPR on accounting practices, we felt it was necessary to determine the level of knowledge of accountants and auditors about this new legislation. In order to do so, we conducted a survey-based analysis. The questionnaire was sent to 200 Romanian accountants, financial and internal auditors, and responses were obtained between the 1st and 15th of March, just over two months before the GDPR went into effect.

The aim of this survey was to assess if accounting and audit professionals are aware of the regulation and have begun to review their practices in light of it.

The questionnaire, which consisted of 11 close-ended and semi-closed questions focusing on the respondents' interpretation of GDPR topics from the accounting activities' perspective, was structured to cover all GDPR topics from the accounting activities' perspective. The participants were also given the choice of selecting from a variety of choices. We tried to keep the number of questions to a minimum in order to prevent any repetitive or well-known responses.

We took into account the fact that numerous responses from practitioners in the same organization would impact the research's accuracy when sending out the survey. As a result, when sending the survey invitation, we made an effort not to send it to more than two people from the same organization. We sent the survey out through professional networks like LinkedIn, and we used other professional groups to find potential respondents. We did not ask the participants to name the

companies they work for because we felt it was important to maintain some level of confidentiality.

We received 109 responses during the two weeks that the participants completed the questionnaire, for a response rate of 54.5 percent, and no forms were omitted because all of the forms received were complete and met the study's criteria.

The respondents' professional experience ranges from one to more than five years, with the majority of 36.7 percent having between two and five years of experience, 33 percent having more than five years of practical experience, and the remaining 30.3 percent having between one and two years.

Furthermore, the participants work for businesses of various types, based on the number of workers, such as small businesses, which made up the bulk, medium-sized businesses, and large businesses. The distribution of respondents' responses to company size can be seen in the graph below.

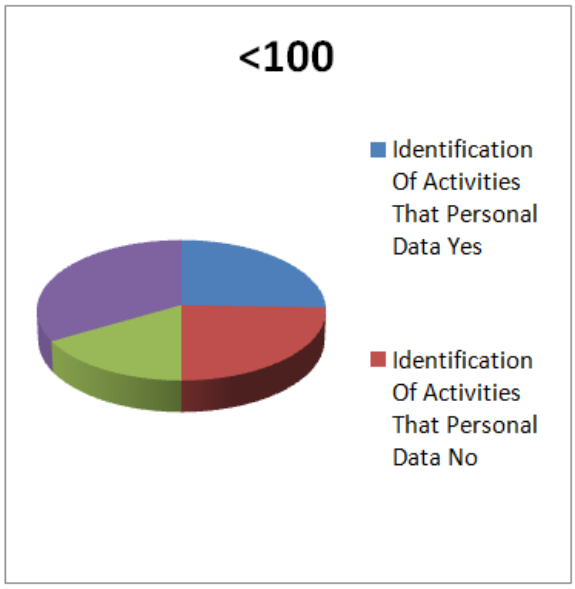

Figure 1

STUDY RESULTS AND DATA ANALYSIS

We discovered that 51.37 percent of the respondents are members of accredited registered national and international accounting and audit societies based on the responses we got. As stated in the previous section of this paper, professional associations have begun to provide a foundation for all individuals within and outside of organizations to obtain a better understanding of the effects and potential actions during the GDPR implementation.

Participants were also asked whether they work with some type of personal data, such as full names, social security numbers, bank account numbers, or any other details that could contribute to an individual's identity, as described by the GDPR system. The fact that more than 83 percent of respondents are working and storing such information has been highlighted after reviewing the responses.

Another question in the survey asked whether the participants were aware of the legislation, and the results revealed that only 61.5 percent of the participants were. The discrepancy is important because we performed a more in-depth survey, which showed that of the 83 percent of people who deal with personal data, 35 percent were unaware of GDPR until the moment they took part in the research, while 44 percent of those who said they don't use personal data

reported their knowledge of the regulation. However, it's important to note that this research was done two months before the GDPR went into practice in Romania and the rest of the EU.

Due to the fact that we are primarily interested in the possible impact of GDPR and attempting to assess practitioners' levels of expertise, we will begin our study with only those respondents who stated that they do use personal data.

When asked if their employers told them about the law, more than 35.15 percent said yes, 24.17 percent said they hope to be informed shortly, and 40.65 percent said they don't know if they will be informed or not. When we looked into this further, we discovered that of the 40.65 percent of respondents, 35.17 percent operate in businesses with more than 250 workers. Employees in small and medium enterprises account for the bulk of the workforce. Given that the majority of respondents said their businesses had not yet told them about GDPR, we believe this is worrying, particularly given that it may take some time for organizations to establish a clear structure and define and comply with personal data processing activities. Nonetheless, we anticipate a reduction in these disparities in the foreseeable future.

The survey's next two questions centred on the practitioners' key behaviours that necessitated the use of personal data. When asked if they were able to find out, they said yes. So far, only 52.74 percent of those who come under the GDPR regulation have begun to recognize and define those behaviours, while the remaining 47.26 percent have not. In addition, the survey asked if the practitioners checked their job processes for certain tasks, and the results revealed that only 37.36 percent of the participants said yes. We can see how, as our study progressed, the information gap widened, emphasizing a troubling lack of understanding and action plans. Nonetheless, after comparing these findings with the company size, these results can also be clarified by the company size. , we discovered that the majority of respondents who reported that procedures had not been revised work in businesses with fewer than 250 workers, where the effect of GDPR might be less severe if their primary activities are not dependent on the processing of personal data.

The table below provides more information about the composition of the responses as they apply to the scale of the firms.

Table 1: Based on the Scale of the Firms, The Distribution of Responses

No. of Employees	Identification of Activities that Personal Data		Reviewing the Policies of the Activities that the use Personal Data	
	Yes	No	Yes	No
<100	23	22	15	30
In between 100 to 250	13	8	7	13
>250	15	16	15	16
Total	51	46	37	59

As can be seen from the table above, there is a difference between the recognition of activities and the actual revision of work procedures in small and medium businesses, while the pattern in large businesses are stable. Nonetheless, the finding can be explained by the fact that, in comparison to other forms of businesses, large corporations typically keep a full record of their operations and practices and have a higher degree of segregation.

So far, based on the survey results, we may conclude that there is a clear awareness gap in Romania when it comes to GDPR implementation, as professionals are not adequately trained and their practices are not thoroughly monitored to ensure compliance with the regulation. However, we must bear in mind that there are still a few months before the compliance date, so a reduction in the gap is expected.

We asked the participants to respond to a query about the security steps they are taking to keep their data safe, as we did in the previous section of the paper about the proper ways in which accountants should comply with GDPR. The findings are depicted in Figure 2.

As can be seen from the graph, the respondents' preferred approach is to change their password on a regular basis, which is typically a necessity in the majority of today's systems. However, the participants' second option demonstrates that they are beginning to increase the security of their accounts, whether due to password combination constraints or not, which is a positive point. In view of recent ransom ware attacks, the third alternative could raise a red flag. Nonetheless, this finding reinforces the Verizon finding, concluding that accountants are highly insecure. Securing attachments when sending by email is a safe practice to prevent a man-in-the-middle attack, but as the chart shows, only a small percentage of professionals use this strategy.

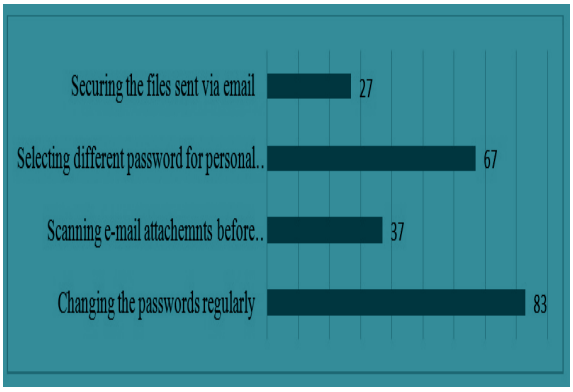

Figure 2

Despite the fact that the list we presented is not entirely complete, no other responses have been received, despite the fact that the participants had the option of including some other security methods besides the above four. This gives the impression that they are still learning about the security measures and the potential implications of security breaches.

FINAL THOUGHTS

After reviewing the possible effect of the GDPR regulation on accounting activities, we were able to identify the key areas where adjustments in key accounting activities centred on personal data processing could occur. As previously stated, professional associations are attempting to provide adequate support to practitioners in order for them to comply with the regulations. However, enforcement would not be feasible without the cooperation of the organizations for which the practitioners operate, as well as a smooth partnership with IT departments, as full and total compliance necessitates efficient collaboration with all departments involved in the process in the fields of data collection, accounting, and human resources.

After conducting an empirical study to determine the level of GDPR awareness among Romanian accountants and auditors, the findings revealed a strong knowledge gap between actual practice and expectations. However, before the deadline on May 25, 2018, there is still time and space for progress. Furthermore, after examining the accountants' practices in order to safeguard their operations, it was discovered that they do not completely comprehend the methods for securing personal and private information, as their conduct has yet to be enhanced.

Since this research was performed just a few months before GDPR implementation, the authors foresee a reduction in the information gap to be found in the immediate future, closer to the regulation's implementation deadline. Nonetheless, we anticipate an overall improvement in accounting security standards as a result of GDPR, which will not be limited to personal data processing.

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/ corp. orate/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], [Retrieved at February 28, 2018] http://www.accaglobal.com/content/dam/ACCA_Global/ Technical/Future/pi-ethics-trust-digital-age.pdf*

12. *Verizon (2017), "2017 Data Breach Investigations Report", [Online] [Retrieved February 28, 2018]*
13. *https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf*
14. *Villaronga, E. F., Kieseberg, P., & Li, T. (2017), 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten', Computer Law & Security Review*
15. *Wachter S., Mittelstadt B. and Russell C., (2017), "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR", Working paper, [Online], [Retrieved March 1, 2018] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289*
16. *Zerlang, J. (2017), 'GDPR: A Milestone in Convergence for Cyber-Security and Compliance', Network Security, (6), 8-11*