THE USV ANNALS OF ECONOMICS AND PUBLIC ADMINISTRATION | VOLUME 19, ISSUE 2(30), 2019

GDPR AND ITS IMPACT ON IT DEPARTMENTS OF COMPANIES

Professor PhD **Doru TILIUȚE**
„Ștefan cel Mare" University of Suceava, Romania
dtiliute@seap.usv.ro

Abstract:
Since May 2008 applying EU GDPR regulation became mandatory for all member States. The aim of the GDPR (General Data Protection Regulation) is to protect all EU citizens from privacy and data breaches in today's data-driven world. The (GDPR) is considered being the most important change in data privacy regulation in the last 20 years. As a consequence, all public institutions and private companies operating with personal data are obliged to fully comply with the requirements of the GDPR. As long as the data processing is automated and many information is collected in electronic format, the IT&C sector is deeply involved in assuring the fair level of personal data protection. The present paper aims to show some action to be taken by the management regarding the IT department within firms and institutions, in order to comply with GDPR regulation.

Key words: GDPR, privacy, personal data, EU regulations.

JEL classification: K22, M15, M21, M48.

1. INTRODUCTION

More and more companies and institutions collect and process data on the people they interact with, starting with the HR department, continuing with the educational institutions and the fiscal ones to the big traders. Regardless of how the data are collected: in physical form - on printed paper or electronically, they are processed and stored almost exclusively in electronic format. Usually the data is stored distributed, according to their source and nature; the data regarding the employees are not in the same place with the data of the clients nor with those for the business analysis. This data distribution and the fact that they cross the institution's computer network, being accessed from different places from where they are stored, further exposes the data of the risk of being stolen and used illegally. According to The Breach Level Index [1], 70 records are stolen or lost every second that leads to 6,034,284 records by day. Among all breaches, only 4% were "Secure Breaches" where the data encryption was used and the stolen data was rendered useless. According to the cited source, the top 10 most severe breaches reported in 2018 are displayed in

Table 1.

Table 1. Top 10 most severe breaches in 2018

Rank	Risk Score	Industry	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location
1	10.0	Social Media	2,200,000,000	04/04/18	Identity Theft	Malicious Outsider	USA
2	9.8	Hospitality	383,000,000	09/08/18	Identity Theft	Malicious Outsider	USA
3	9.5	Other	200,000,000	07/01/18	Identity Theft	Malicious Outsider	USA
4	9.3	Hospitality	130,000,000	08/28/18	Identity Theft	Malicious Outsider	China
5	9.1	Other	340,000,000	06/01/18	Identity Theft	Accidental Loss	USA
6	9.1	Retail	150,000,000	02/01/18	Account Access	Malicious Outsider	USA
7	9.0	Social Media	336,000,000	05/03/18	Financial Access	Accidental Loss	USA
8	8.9	Other	180,104,892	11/12/18	Identity Theft	Accidental Loss	Brazil
9	8.9	Social Media	100,000,000	11/30/18	Account Access	Malicious Outsider	USA
10	8.7	Other	113,500,000	09/01/18	Identity Theft	Accidental Loss	USA

It can be seen that the highest score belongs to Social Media industry, whose number of breached rerecords exceeds the sum of all other industries. The risk Score for Healthcare and Education is lower but still considered "critical",

Table 2 and Table 3. Even if the occurrence of the United States in the statistics is higher, other states have registered a higher number of breached records, with a higher degree of risk.

The order of the industries, in terms of risk, changes from year to year and for a long time the technology was in the first places. Only in recent years, with the proliferation of Social Media, this one has reached the first place. Table 4 shows the first 12 positions since 2016.

Table 2. Top 5 Risk Score in Healthcare industry

Rank	Risk Score	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location
31	7.7	3,000,000	01/18/18	Identity Theft	Malicious Outsider	Norway
42	7.4	1,500,000	07/04/18	Identity Theft	Malicious Outsider	Singapore
44	7.4	1,400,000	03/14/18	Identity Theft	Malicious Outsider	USA
45	7.4	1,400,000	03/14/18	Identity Theft	Malicious Outsider	USA
53	7.1	3,500,000	03/14/18	Identity Theft	Accidental Loss	USA

Table 3. Top 5 Risk Score in Education

Rank	Risk Score	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location
39	7.6	10,300,000	06/09/18	Identity Theft	Accidental Loss	Malaysia
63	6.9	500,000	01/01/18	Identity Theft	Malicious Outsider	USA
71	6.7	301,148	09/18/18	Identity Theft	Malicious Outsider	Spain
78	6.6	1,097,000	01/22/18	Identity Theft	Accidental Loss	USA
102	6.2	360,00	02/26/18	Identity Theft	Accidental Loss	USA

Table 4. Ranking of industries, by risk, starting with 2016

	2018		2017		2016	
Rank	Industry	Percentage	Industry	Percentage	Industry	Percentage
1	Technology	28.99%	Other	54.41%	Entertainment	28.53%
2	Other	21.12%	Technology	10.73%	Technology	26.68%
3	Social Media	19.70%	Government	9.96%	Government	24.31%
4	Retail	8.33%	Financial	8.81%	Social Media	8.15%
5	Government	7.03%	Professional Services	5.42%	Other	5.89%
6	Financial	3.76%	Retail	5.08%	Retail	2.25%
7	Hospitality	3.59%	Social Media	1.51%	Healthcare	1.84%
8	Entertainment	3.41%	Healthcare	1.33%	Financial	0.87%
9	Healthcare	1.98%	Entertainment	1.30%	Hospitality	0.65%
10	Professional Services	1.00%	Education	1.29%	Insurance	0.63%
11	Education	0.85%			Education	0.16%
12	Industrial	0.14%				

All tables before shows clearly that there are not industries to not be affected by data security issues and in these conditions IT&C departments need to play a much more important role in protecting sensitive data held by the organization in order to comply with GDPR requirements.

2. TYPES OF VULNERABILITIES

From the very beginning we should say that in the process of implementation and compliance of the GDPR, the responsibility is not entirely of the IT&C compartment, although it plays a very important role in this plan; the overall responsibility belongs entirely to the management of the institution, which must have an integrative vision on all the aspects that the Regulation refers to.

Among the vulnerabilities faced by the personnel of the IT department we mention: Quality of data storage and handling, staff awareness and training, computer network security, audit of GDPR compliance.

Data storage and handling

One of the most challenging problems for the IT&C department is the fair management of the access to systems storing personal data and how they are processed. This problem is, actually, a bunch of sub-problems as follows:

Who and in which conditions has access to data storage systems? Ideally, all data should find centralized servers, restricted and logged access. In fact, in many institutions or companies, personal data is distributed on several client computers, where access is less controlled and the management of the computer is done by the operator himself. This situation is closely related to another problem, that of awareness and training of the personnel who owns and operates such data. Until the problem of data centralization is solved, the access to the client computers must be password protected and after short periods of inactivity, the system must requires a re-authentication of the user. In the desired situation, where the data are centralized on servers, they must be located in special rooms, where the access is strictly regulated. Only the personnel with clear responsibilities in the administration of the servers must have access in the respective rooms, based on access codes or biometric identification. The date and time of entry, the duration of intervention, the persons who have intervened, must be recorded in log files, to which only the head of the department and the management of the organization have access but only in read mode.

Because the access to data can also be done remotely, through the institution's network, it must be restricted by credentials and also logged. Different levels of access should apply to the employees of the IT&C department, depending on their role in the systems administration.

How safe is the remote access? Administrators of information systems usually use the remote access to these systems. Because sensitive data are transmitted between administrator’s computers and servers, the connections must be secured. For this purpose, only encrypted connections with strong encryption systems, will be used. Encryption ensures that the data exchanged between data terminals remain unintelligible and useless to potential attackers. Using a Virtual Private Network (VPN) for systems administration is a good practice in order to prevent possible indiscretion of regular users.

How safe are the applications? There are not infallible software application in terms of security. Beside the vulnerabilities that are found in enterprise applications, web-based applications are prone to attacks such as Cross-site Scripting (XSS), SQL injection, etc. Consequently, this sort of applications should be tested specifically for those types of attacks for which they are most vulnerable [2].

Many applications store date in plain text format, because this practice simplifies application design and makes information extracting process easier and quicker as well. However, storing data in this way expose information to the possible attacks. In order to mitigate the risk of personal date

disclosure, GDPR recommends using *encryption*, *pseudonymisation* and *anonymization* of information [3].

In a simple definition, "encryption is the conversion of data from a readable format into an encoded format that can only be read or processed after it's been decrypted" [4]. Beside the plain text and encrypted text, cryptography operates with encrypting algorithms and keys. As a general rule, the longer encryption key is and the more sophisticated is the algorithm, much stronger the encryption is. If there is a need for recovering information in plain format, then symmetric encryption algorithms must be used, but this may affect data security if an attacker comes in the possession of the key and knows the algorithm being used.

According to Article 4, item 5, in GDPR, "pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". Pseudonymisation is useful when data are important and must be kept in a readable format, but it cannot be and must not be associated to a real person.

In some conditions the pseudonymisation may lose its role in protecting personal data information. For instance, in figure1 we show a very simple way to "hide" the real name of a person, by replacing the letters with the next ones in the alphabet. Spaces are replaced by special characters, as ?,*,!,# etc. Anyone knowing the method we used to not revealing the real name, can find it out by applying the method in the reverse order. That's why an important requirement of the pseudonymisation is too keep secret the algorithms being used by the Data Operator.

Figure 1. Pseudonymisation of a name, by replacing a character with the next one in the alphabet.

Anonymisation is a much efficient method, in which there is no way to associate personal data with a specific person. Data are kept in a readable format, suitable for further processing, but any information which can lead to the identification of the person are either eliminated either encrypted using one-way strong algorithms [5].

Staff awareness and training

Although it seems hard to believe, the employees are responsible for a large number of security incidents with major consequences for companies. According to the *Verizon 2018 Data Breach Investigations Report*, "20 percent of cybersecurity incidents and 15 percent of the data breaches investigated in the report originated from people within the organization, with financial gain and pure fun being the top motivators" [6].

Within the risks generated by the employees, we mention only six:

Malicious or Disgruntled Insiders – are the employees (many having IT knowledges) disgruntled by their salary or job conditions or motivated by external financing which steal data, code, intellectual property, and other sensitive information. For this purpose they use a different type of tools such as email, USBs, FTP, screen shots, and mobile devices to pursue their nefarious goals [7].

Accidental Misuse of IT Assets is the result of the accidental or voluntary action of the employees who violate the rules of behavior in the workplace. This behavior include copying date from the company computers onto the me memory stick, using unauthorized tools for accessing work email from another location, downloading media files from uncertain servers and so on.

BYOD Devices is a vulnerability produced by bringing of personal IT devices at the workplace (Bring Your Own Device). Using those devices to access company information, to copy and share files expose the company to high risks, because the devices might be infected with malware or running unpatched software vulnerabilities.

Phishing attacks and Social media, are some of the greatest IT security risks to organizations as for the individuals. Phishing is a kind of attack in which an imposter sends emails to the potentially victims, tricking them to click on malicious attachments or links. In recent years, such links or misleading ads are increasingly distributed on social networks. If the victims click on the fake links or ads, they are led to a webpage looking like the original (but isn't) and are asked to enter confidential information, such as credit card numbers, Social Security numbers, etc. Because phishing attacks becomes more and more sophisticated, creating the illusion of the authenticity of messages and advertisements, the staff must be very vigilant and suspicious of anything. Otherwise, with a simple click, an unsuspecting employee could reveal their credentials and grant attackers access to the corporate network.

According to the Verizon's Report in 2016, 30% of phishing messages were opened by the target across all campaign which indicates a significant rise from the previous year's report (2014) in the number of folks who opened the email (23%) [8].

Weak Passwords are another important source of vulnerabilities. Short passwords or password based on common words or phrases are easy to guess, so they must be long enough and contain characters generated randomly. In many situations employees need to access multiple online accounts frequently and it is very difficult for humans to keep in mind strength passwords meeting the above requirements. As a consequence, the passwords are weak and if they are not changed frequently, the back door is as open. Any organization might require their employees to frequently change their passwords in order to strengthen the security of those accounts.

Installing Rogue Programs is a quite common phenomenon and consists of unauthorized installation by employees of programs from dubious sources. Programs from uncertain sources may contain viruses or malware that might make the organization's systems vulnerable sending credentials or documents to a third party. The regular users should not have administrative rights on their computers so they will never will be able to make changes on the computers, including installation of new software.

In order to reduce and prevent the risks produced by employees, it is necessary for the organization to periodically organize training sessions, in which employees are reminded of the rules to follow in the company, what are their rights and obligations, as well as the security incidents that occurred in the past and their causes. Phishing attacks simulation can bring interesting information about how employees respond so that the results are used in training sessions.

According with the GDPR, employees who process personal data must sign a confidentiality agreement with the company where they work, which can make them more aware of their actions.

The employees in IT department must supervise how other employees use their computers at work, reduce or suppress administrative rights on the computers and report any security incidents to DPO.

Computer network security

When people access personal data in electronic format, data travel through the computer network from the storage location to the end user. The network consists not only in cables but in a lot of equipment where they can be intercepted and further used in illicit purpose. Therefore, these equipment, whether they are routers or switches, must be protected in secure enclosures, with controlled access. On the other hand, data must be encrypted when it transits the computer network, even though it may appear as plain text to the end user. This makes data unusable, even in the case of interception.

Wireless networks are more vulnerable than wired networks, despite the advances in securing them with increasingly complex protocols. Under no circumstances will open **WI-FI**

networks be used to carry sensitive data, and in secure networks this will be avoided as far as possible.

All computers in the network will be registered with the IT department and other computers, unauthorized, will not have access to the network. The use of employees' personal computers at work must be strictly regulated and even these computers must be registered in order to prevent unauthorized access to company data.

Audit of GDPR compliance

GDPR is quite new and it rises many difficulties in ensuring the full compliance. Even the audit firms, which have appeared in response to the obligation to comply with the GDPR of all organizations operating in the EU, are experiencing problems in assessing the situations they encounter. However, as specialized firms, which accumulate experience with each audit mission, the audit firms are key resources in helping enterprises achieve and maintain compliance.

A check point in GDPR audit checklist is ISMS (Information Security Management System). The aim of ISMS is to find out if there are appropriate technical and organizational measures in place to ensure the adequate security of personal data held in hard copy or electronic form, or processed through the information systems. The audit includes, among others, the review of security testing methodologies and the existence of certifications, compliance with established cyber standards and codes of practice.

In this regard, the implementation of the international standard ISO 27001:2013 is very useful, because the standard complies both with the EU GDPR and the NIS Regulations (Network and Information Systems Regulations) [9].

CONCLUSIONS

The GDPR is a very serious problem, even just after the size of the fines applied in case of non-compliance. The maximum fine rise up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher, for the infringement of the articles regarding: the basic principles for processing; the conditions for consent; the data subjects' rights and the transfer of data to an international organization or a recipient in a third country. That is why companies have spent and continue to spend large amounts to comply with all GDPR requirements, which are not easy to meet.

REFERENCES

[1] „Breach Live Index," 2018. [Interactiv]. Available: https://breachlevelindex.com/. [Accesat 06 09 2019].

[2] „GDPR and Penetration Testing," 15 April 2019. [Interactiv]. Available: https://www.breachlock.com/gdpr-and-penetration-testing/. [Accesat 09 September 2019].

[3] E. Commision, „Data protection in the EU," 2016. [Interactiv]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. [Accesat 09 September 2019].

[4] K. Lab, "What is Data Encryption?," [Online]. Available: https://www.kaspersky.com/resource-center/definitions/encryption. [Accessed 22 August 2019].

[5] Data Protection Commission (DPC), „Guidance Note: Guidance on Anonymisation and Pseudonymisation," June 2019. [Interactiv]. Available: https://www.dataprotection.ie/sites/default/files/uploads/2019-

06/190614%20Anonymisation%20and%20Pseudonymisation.pdf. [Accesat 19 September 2019].

[6] S. Shepard, „Verizon Report Explores the World of Insider Threats," June 2019. [Interactiv]. Available: https://securitytoday.com/articles/2019/03/06/verizon-report-explores-the-world-of-insider-threats.aspx. [Accesat 19 09 2019].

[7] D. Bisson, „10 IT Security Risks Your Employees Bring to Your Organization," Meta Compliance, 16 08 2016. [Interactiv]. Available: https://www.metacompliance.com/blog/10-it-security-risks-your-employees-bring-to-your-organization/. [Accesat 19 09 2019].

[8] "2016 Data Breach Investigations Report," 2016. [Online]. Available: https://regmedia.co.uk/2016/05/12/dbir_2016.pdf. [Accessed 10 08 2019].

[9] "The Directive on security of network and information systems (NIS Directive)," 07 2016. [Online]. Available: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. [Accessed 09 2019].