CHALLENGES IN ELECTRONIC COMMERCE FROM THE ASPECT OF PROTECTING PERSONAL DATA STORED IN CERTAIN DATABASES AND DIGITAL FORENSICS

Snežana Stojičić[1]
Nataša Petrović
Ministry of the Interior of the Republic of Serbia

Vojkan Nikolić, PhD
Radovan Radovanović, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Abstract: It is incomprehensible that the digital era is increasingly developing and applying electronic business. The use of electronic data stored in certain databases, electronic communications and electronic processing of large amounts of data in the performance of business processes of natural and legal persons is evidently increasing, in response to the challenges that electronic business brings, development and harmonization of the normative framework as in the domain of increasing the efficiency of business as well as the challenges that the digital era carries with it especially from the aspect of protection of personal data. The new European Data Protection Regulation (GDPR) has been in place since May 2018, while implementation at the national level begins in the second half of 2019, experience and challenges are the subject of current considerations. The challenges posed by the implementation of the normative framework must also be followed from the forensic aspect in response to potential violations and non-compliance with legal norms, which requires the development and application of new procedures and tools in this area. It is also evident that there is a need to raise the level of knowledge in this field, bearing in mind the specificity of the relation between the normative and technological aspect and the research that is being carried out in this field, both from the aspect of consideration and confidence in the reliability of the application of electronic commerce from the aspect of obtaining and processing information related to forensic aspects in the digital world. The topic of the discussion are precisely these issues that relate to the challenges in electronic commerce both from the aspect of protection of personal data and from the aspect of digital forensics.

Keywords: electronic business, personal data protection, digital forensics, ICT systems, databases

1 snezana.stojicic@mup.gov.rs

INTRODUCTION

Together with the increasing digitization of data and the increased application of the ICT System, it is an evident increase in the use of the electronic business. Also, personalization of the services occurs in all domains ranging from the use of services and e-services in certain sectors, such as banking, up to e-Government services, and this leads as well to an increase in the collection and processing of personal data. Personal data can be found in various data records, which are the most often collected, stored and provided for further use even under a much stricter procedure. With the evident increase of the applying and using of new electronic services, the importance of protecting personal data in field covered by electronic business, arise continuously. This result with needs to responding improvement of normative framework at EU level and beyond which was followed by adopting the General Data Protection Regulation is widespread. The General Data Protection Regulation – GDPR (Regulation (EU) 2016/679, Official Journal of the European Union, 2016) was adopted by the European Parliament in April 2016, and has been in effect since May 2018. It has been designed to protect the data of EU citizens and its implementation affects every single organization and business that interacts with an EU resident, regardless of where they may be. It is the most important change in data privacy regulation recently adopted, and fundamentally reshapes the way in which data is handled and has made significant changes in all sectors applying electronic bossiness principle. Furthermore it harmonizes practice regarding personal data processing with ICT systems and services. Especially having in mind that the regulation does not apply only to companies EU-based, but also to companies with headquartered outside the EU that place their products or services in the EU.

The modern digital environment creates new challenges and opportunities for perpetrators of criminal acts, as well as services that influence the illumination of these. So the process of digitization and modernization of business processes is necessary to monitor the development of an adequate response from the aspect of digital forensics. Digital forensics, as one of the branches of forensic science, which aims to gather and document evidence in electronic form, put them in adequate databases and search and explore data using digital forensics and techniques based on information and communication technologies.

Items subject to the Code of Criminal Procedure must be seized or may serve as evidence in criminal proceedings also include automatic data processing devices and devices and equipment on which electronic records are stored or can be stored (Code of Criminal Procedure ("Official Gazette RS, 2011). In the processes of conducting an investigation by digital forensics techniques, collecting, analyzing and presenting digital evidence, it is necessary to ensure that they comply with the normative framework, presented clearly and comprehensively, consistent and acceptable, ensuring the integrity of all types of evidence in digital form.

GDPR SCOPE

The general regulation on the protection of personal data is the response to the increasing representation of new technologies in everyday life, the increasing importance of processing personal data in contemporary economics, national security, scientific research and technological development, as well as reducing confidence in new technologies and their use in the public and private sectors. It relates to the protection of individuals with regard to the processing of personal data and rules related to the free exchange ("movement") of such data within the European Union, as such applies in all Member States, the harmonization of regulations concerning the protection of personal data at the level of the European Union, and beyond, bearing in mind that it does not apply only to EU-based companies, but also to companies headquartered outside the EU that place their products or services in the EU. It applies to the processing of personal data that is fully automated, as well as to non-automated processing of personal data that form part of the recording system or are part of the data recording system.

Primary emphasis is on the scope of application, and no less important is that this regulation does not apply to the processing of personal data: during an activity that is not covered by the legal framework of the European Union, carried out by a natural person during solely personal or household activities and performed by the competent bodies in the purpose of preventing, investigating, detecting or prosecuting criminal offenses or the execution of criminal sanctions, including the protection of public security.

Determination of the concept of personal data has been extended in relation to the previous normative framework (EU 95/46/EC) or a person who can be identified directly or indirectly (name, identification number, location data, network identifier or with the help of one or more characteristics of the inherent for the physical, physiological, genetic, mental, economic, cultural or social identity of a particular person).

Figure 1. *Basic principles of the General Regulation on the protection of personal data*

The principles of personal data processing (Figure 1) relate to a lawful, appropriate and transparent way of processing, right for the data to be collected and processed in accordance with the legally defined purpose, minimizing the use of personal data only to relevant and limited with what is necessary in relation to the purpose according which they are processed, the accuracy and the timeliness of the data, as well as the measures to be taken without delay, in the case of data in relation to the purpose for which they are being processed, are not correct (correction or deletion), limit the retention in accordance with the purpose for which personal data is processed, unless personal data is processed for archival purposes, in the public interest, for the purpose of the scientific or historical research or for statistical purposes, with the application of appropriate safeguards and guarantees of data integrity.

GDPR BRINGS

The new regulation also introduces the concept of pseudonymisation which refers to processing that is done in a manner that prevents the attribution of personal data to a particular person without the use of additional information or data. The application of pseudonymisation to personal data can reduce the risks of violation of data protection obligations. It can be provided in such a way that this additional information for attributing the personal data is kept separately. Furthermore, technical, organizational and personnel measures have to be taken to ensure that personal data cannot be attributed to a particular or specific person. Pseudonymization would mean that data are converted in such a way that the personal data cannot be detected by a reversible process.

The concepts Privacy by Design and Privacy by Default or the concept of integrated privacy protection (Privacy by Design) are being introduced, i.e. that the integration of elements related to the protection of personal data is considered from the design phase of the ICT System and databases development up to the production work and use of developed solutions. In any case, privacy policies should be written in a simple and comprehensible way to the end user. Also, the user should clearly state the consent before access to the use of personally identifiable information, i.e. silence. Pre-marked field or non-response cannot be considered as consent. Consent should be given a clear and affirmative act that expresses the voluntary, independent, informed and unequivocal consent of the person to whom the data relate, in relation to the processing of personal data. The user must be informed about the purpose for which the information and data are collected, stored in specific databases and processed. Moreover, the user has to be informed about the automation of the procedure, as well as about the possibilities of disputing further processing.

It is obligatory to inform users in the event of data breaches occurring in specific databases, without delay or up to the prescribed deadline (Figure 2).

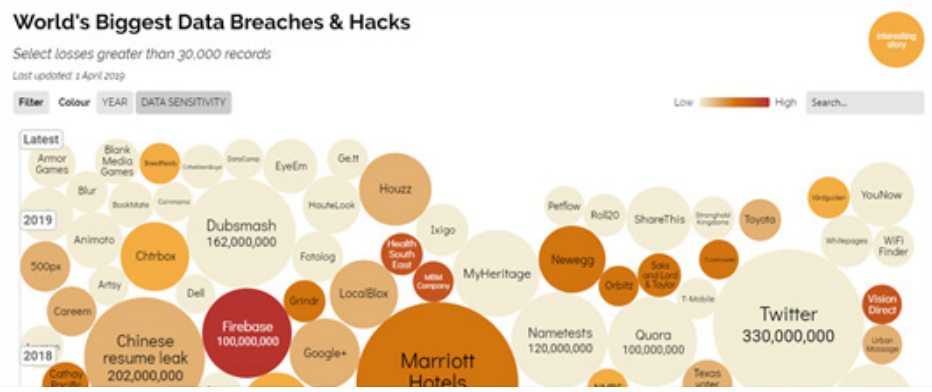

Figure 2. *The biggest cases of violation of records and personal data in the world*[2]

However, there is a general principle for transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization. It provides the possibility of transferring personal data which shall take place only if, subject to the other provisions of the GDPR and means that personal data from one database may be transferred to another using the web service. Also there is a defined principle regarding when the right of access can be used to obtain a copy of the data that is being kept on the person, as well as the right to revoke the consent previously given for the processing of personal data, or delete data from certain databases.

Certain public attention has attracted high penalties that can be imposed by data protection authorities, which are supposed to be up to € 20 million or 4% of annual turnover.

The General Regulation on the Protection of Personal Data provides methodology for the reporting and mechanism how it has to be implemented. The first report and revision will be implemented by 2025, and thereafter periodically every four years. The European Commission, if necessary, submits appropriate proposals with a view to change the GDPR regulation, especially taking into account the dynamics and trends in the development of information and communication technologies, as well as the development of the information society as a whole.

THE YEAR OF THE APPLICATION OF GDPR

The new rules require that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand. Clear and plain language has to be used or additionally, where appropriate, visualisation can be used. Companies have to use simple explanations of the way how the data will be

2 *https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*

managed and handled, mandatory requesting data collection and storage of certain data in databases, ensuring the possibility of copying data to users or deleting them on demand, as well as reporting data security breaches. Many companies already have been harmonized with the GDPR regulations during the first year of implementation, although there have also been those who have been subject to penalty provisions with significantly high penalties. Google is one of the examples. It was penalized with around 50 million euros during this first year of application[3]. In preparation for the implementation of the GDPR regulation, some large companies such as Apple and Facebook have developed new user tools to be able to control and/or delete the collected data.

However, for a year in the implementation of the GDPR, things generally take place well in line with the GDPR regulations. According to the International Association of Privacy Professionals (IAPP[4]), organizations have set up their privacy teams and are making efforts to implement the GDPR regulation in most cases. Since May 2018, more than 95,000 citizen complaints have been registered with the Data Protection Authority (DPA), most of the complaints, it can be said relates to electronic commerce, video surveillance and similar cases[5]. What can be assessed as a major contributor to the implementation of the GDPR Regulation is transparency in terms of data security breaches. In 2018, only 1,700 data security injuries were reported, while estimates that approximately 36,000 data security injuries will be reported in 2019.

According to a study released by law firm DLA Piper[6] from London, around 60,000 data security injuries in the first eight months of the implementation of the GDPR regulation were reported across Europe. According to research conducted in the US by TRUSTe / NCSA, 92% of Internet users expressed concern about privacy in the online environment, 89% avoid companies that do not have a privacy policy, and 60% think privacy in the online environment should be human rights[7] . Trust in e-commerce plays an extremely important role, and is a challenge in the development and use of services and electronic services, as well as the topic of many of the world's research.

According to research conducted in the UK by the International Commissioner's Office - ICO, in June 2018, about a third (34%) of interviewed citizens declared that they had great confidence in companies and organizations that have and use personality data, which represented a significant increase compared to 2017 when this opinion was about 21%. In a survey conducted in March 2019, 64% fully agree or agree with the observation that progress is visible in relation to individual rights in relation to the collection and processing of personal data compared to May 25, 2018, when the application of the GDPR Regulation began.

3 Lineate tech solution company - *https://lineate.com/gdpr-one-year-later/*
4 The International Association of Privacy Professionals - The world's largest global information privacy community
5 *https://www.lexology.com/library/detail.aspx?g=e6416273-7c56-456c-b102-991dcde14991*
6 *https://www.dlapiper.com/en/europe/focus/eu-data-protection-regulation/home/*
7 *https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/*

GDPR IN SERBIA

The Law on Personal Data Protection[8] was adopted on November 9, 2018, with a delay of nine months for its implementation. Bearing in mind the ongoing process of Euro integration, the preparation of the law took into account compliance with the General Regulation on the Protection of Personal Data and Free Data Flow, Directive 2016/680, and Directive 2016/681. The Law on Personal Data Protection regulates the right to protection of natural persons in relation to the processing of personal data and the free flow of such data, the principles of processing, the rights of the persons to whom the data relate, the obligations of the handlers and processors of personal data, the code of conduct, personalities in other states and international organizations, supervision over the implementation of this law, legal remedies, liability and penalties in case of violation of the rights of natural persons in relation to personal data processing, as well as special cases of processing. This law also regulates the right to protection of natural persons with regard to the processing of personal data by the competent authorities for the purpose of preventing, investigating and detecting criminal offenses, prosecuting offenders or enforcing criminal sanctions, including prevention and protection against threats to public and national security, as well as the free flow of such data.

Personal data protection is provided to any natural person, regardless of nationality and residence, race, age, sex, language, religion, political and other belief, nationality, social status and status, wealth, birth, education, social status or other personal properties. The data must be adequately protected against misuse, destruction, loss, unauthorized changes or access (Law on Personal Data Protection, Official Gazette RS, 97/2008)[9].

Personal data breach can be considered as a security incident in which data that is protected or restricted access, accessed, reviewed, copied, transferred or used by a third party that is not authorized. While an incident can be considered as any event that is not part of the standard functioning of the service and which causes, or can cause, interrupt and decrease the quality of that service.

The rules relating to the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or the enforcement of criminal sanctions, including protection against threats to public safety and their prevention are defined by Directive (EC) 2016/680[10]. Accordingly, Member States protect the fundamental rights and freedoms of individuals, and in particular

8 *http://www.parlament.gov.rs/upload/archive/files/lat/pdf/zakoni/2018/2959-18-lat.pdf*
9 Law on Personal Data Protection ("Official Gazette of the Republic of Serbia", No. 97/2008, 104/2009 - Dr. Law, 68/2012 - decision US and 107/2012)
10 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

their right to the protection of personal data and ensure that the exchange of personal data between competent authorities, where such exchange is required by the law of the EU or the law of a Member State, is not limited to the prohibition in reasons related to the protection of the person regarding the processing of personal data. Also, this Directive sets out the rules relating to the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or enforcing criminal sanctions, including protection against threats to public safety and their prevention. The obligation to protect the fundamental rights and freedoms of individuals, and in particular their right to the protection of personal data, and to allow the exchange of personal data between competent authorities within the EU, where such exchange is based on EU law or the law of a Member State, reasons related to the protection of individuals in terms of data processing of personal data.

GDPR AND DATA BREACH WARNING

In a very short time it is necessary to find sources of digital evidence. Evidence is collected in a mode of work that corresponds to forensic methods and analyzes data breach on site. The data collected is then analyzed and a safe solution is found to overcome the resulting data breach.

Within a few hours, it is necessary to repair the functionality of the disturbed systems and to enable the return of data and functionality of the systems in which the data are processed. According to the GDPR Regulation, after 72 hours of the occurrence of the data breach, it is necessary to provide information related to the subject of the attack and data breach, how it came about, when and from where the data breach began.

In general, CERT teams, system administrators, forensic teams, legal teams, communication experts, human resources and financial investigations can be involved in responding to an attack on data breach.

If we look at the readiness to respond to incident situations or attempt to violate the integrity of the data, it can also be talked about forensic readiness or readiness to collect and document information related to data breaches. Forensic readiness has a significant role both in terms of incident prevention and in response to incidents.

Bearing in mind the increasing scope of where e-business could be applied in modern life and work, it is necessary to assume that the incident will occur, even if the risk assessment is with low probability, so that capacity development in this domain must also be continuous, because forensic readiness is a measure of the capacity for incidents prevention, as well as information that have to be provided about events that have already occurred in adequate form for further use as evidence in court proceedings.

Developing forensic readiness develops capacities for interactive learning based on systemic approaches to gathering information over time, analyzing and allowing detection of threats, and ensuring adequate response and actions regarding provision of evidence in adequate form, especially in case of data breach.

GDPR AND DIGITAL FORENSICS

Digital Forensics is a science aimed at collecting, storing, finding, analyzing and documenting digital evidence, or data that is stored, processed or transmitted in digital form.

Digital forensics and cyber incident incidents are the basis for obtaining evidence in electronic form, and certainly include the evidence that contains personal data contained in certain databases, which fall within the domain of the GDPR regulation. If digital forensic methods are being implemented or processed in incidents in the European Union or in the business involving the international community, it is necessary to take into account the application of the GDPR regulation.

The forensics, following strictly defined rules, collect digital media and electronic information suspected of being on the evidence they are searching for, provide them with any changes, find any evidence and analyze in order to reconstruct the activities that have been performed on them, and prepare a report to be used to conduct a trial or an internal investigation at an institution in which data was abused or leaked.

Digital forensics has wide application and is not limited to police, court, and military intelligence activities. The banking sector, insurance companies and companies of various profiles have a need and must be extremely cautious with the personal data of the clients they have, as many companies are causing enormous damage due to industrial espionage and general misuse of the IT system.

When it comes to personal data, all processes and activities related to the application of digital forensic methods represent the processing of data from the aspect of the GDPR regulation, with the necessary application of all aspects of information security.

CONCLUSION

It can be concluded that the normative regulation in the domain of personal data protection has been significantly improved (GDPR One-Year Anniversary, 2019) by the adoption of the GDPR regulation, and that after a year of implementation there are still challenges that require an adequate response and certainly a significant improvement in the application and observance of the rules relating to data protection about personality, which are found in certain databases. The challenge is the development of readiness for adequate responses to incidents in

the cyber space as well as the development of the capacities for the application of digital forensic methods in order to provide valid evidence for the prosecution of criminal offenses that take place in the digital sphere or are involved in any way in the committing criminal offenses. It is encouraging that the number of personal data security violations has increased significantly, which also contributes to the development of readiness for responses to incidents in the digital cyber space, as well as forensic readiness to provide adequate support for the methods of digital forensics to the processing of this type of casees.

Developing awareness of the risks which brings the digital age, effective implementation of regulations and development capacity for the application of digital forensic methods contribute to the overall increase in the use of e-business in practice.

REFERENCES

1. 2016 TRUSTe/NCSA Consumer Privacy Infographic - US Edition, Accessed April 19, 2019, *https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/*
2. Code of Criminal Procedure ("Official Gazette of the Republic of Serbia" 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 and 35/2019)
3. Code of Criminal Procedure, ("Official Gazette of the Republic of Serbia" 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 and 35/2019)
4. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, Official Journal of the European Union, 2016.
5. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Official Journal of the European Union, 2016.
6. DLA Piper - General Data Protection Regulation, Accessed May 2, 2019, *https://www.dlapiper.com/en/europe/focus/eu-data-protection-regulation/home/*
7. GDPR One Year Later: Differences, Similarities, and Lessons Learned, Accessed May 25, 2019 *https://lineate.com/gdpr-one-year-later/*
8. Law on Personal Data Protection ("Official Gazette of RS", No. 87/2018), *http://www.parlament.gov.rs/upload/archive/files/lat/pdf/zakoni/2018/2959 -18-lat.pdf*
9. Law on Personal Data Protection ("Official Gazette of the Republic of Serbia" No. 97/2008, 104/2009 - Dr. Law, 68/2012 - decision US and 107/2012)

10. 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/EC (General Data Protection Regulation), Official Journal of the European Union, 2016.
11. Simeunović, N., Ristić, N., (2013). Digital Forensic Investigation of Manipulation of Accounting Software, INFOTEH-Jahorina, *http://www.infotech.org.rs/blog/wp-content/uploads/radovi2013/111.pdf*
12. Simeunović, N., Ristić, N., (2013). Digital forensics in the function of forensic computing, INFOTEH-Jahorina Vol.12, p.1006-1010.
13. The Status of the GDPR As the One-Year Mark Gets Closer, Accessed April 19, 2019 *https://www.lexology.com/library/detail.aspx?g=e6416273-7c56-456c-b102-991dcde14991*
14. World's Biggest Data Breaches & Hacks, *https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*
15. GDPR One-Year Anniversary: Data Privacy Still Needs Help, Accessed May 29, 2019,
16. https://www.eweek.com/security/gdpr-one-year-anniversary-data-privacy-still-needs-help