UDK 004.056(497.11)
https://doi.org/10.18485/fb_ic4hs.2018.8

IMPACT ANALYSIS OF THE APPLICATION OF THE GDPR REGULATION ON THE FUNCTIONING OF THE INFORMATION AND COMMUNICATION SYSTEM OF THE MOI OF THE REPUBLIC OF SERBIA

Milan GLIGORIJEVIĆ[*], Radosav POPOVIĆ[**], Aleksandar MAKSIMOVIĆ[***]

Abstract: The development of new information and communication technologies brings undoubted benefits to society, as their use allows for a significant reduction in costs, business processes are automated, facilitated and accelerated, various types and amounts of information become available, and communication opportunities are expanding considerably. Simultaneously with the development of new technologies, threats to their security are growing globally, and hence great attention is paid to their adequate protection. The Republic of Serbia has also realized the importance and seriousness of this issue, and has been working very hard to create a sustainable information society in recent times. Coordination needs to be improved, not only at the national, but also at the international level, bearing in mind that many incidents in ICT systems have a cross-border character. Except in certain areas where there are special regulations (protection of classified information, personal data, electronic communications, etc.), there is no obligation to determine the measures that are necessary to take in order to protect the ICT system. Public authorities, persons dealing with particularly sensitive personal data and legal persons performing activities of general interest must increase their resistance to compromising information security, since the tasks that are of great importance and their smooth functioning are increasingly dependent on new technologies. Infringement of information security could cause major disruptions in vital functions and cause significant damage to the state and its citizens. One such system is also the information and communication system of the Ministry of Interior of the Republic of Serbia, which has recently faced a great challenge: How to implement the obligations and responsibilities prescribed by the new GDPR regulations, and on the other hand to provide the same or higher level of protection of the system itself?

---

[*] Assistant Professor, PhD, Academy of Criminalistic and Police Studies, Belgrade, milan.gligorijevic@mup.gov.rs

[**] MoI of the Republic of Serbia, Deputy Head of the Sector for Analytics, Telecommunications and Information Technologies, Belgrade, radosav.popovic@mup.gov.rs

[***] MoI of the Republic of Serbia, Head Specialist, Legal expert for network and information security, CERT Centre, Belgrade, aleksandar.maksimovic@mup.gov.rs

Keywords: information security, information and communication system, GDPR regulation, protection of classified information, personal data protection

1. INTRODUCTION

In the modern era the right to privacy is increasingly enshrined in constitutional and human rights instruments, and, in some cases, a specific right to the protection of personal data is also included. At the same time, privacy and personal data protection are often challenged in the digital era, due in particular to the worldwide proliferation of internet-based communications that are notoriously difficult to police; the rise of data-hungry applications like search engines, targeted advertising platforms or social networks; and the use of various methods of online surveillance by both private and governmental entities. (Lehavi, Larouche, Accetto, Purtova & Yemer, 2016) The alleged borderless nature of digital technology leads to a complicated set of normative and policy questions. These queries relate not only to the adequate scope of substantive balancing between the individual interest in privacy and the potential interest of other private users, commercial entities, and governments in data disclosure, but also to questions of jurisdiction and governance. The dilemma is thus not only one of *how* (or *how far*) privacy and personal data should be protected, but also one of *who* should be in charge of establishing and enforcing the governing legal norms.

In order to meet all these requirements, the European Union drafted GDPR regulation act in 2016. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). (Blackmer, 2016) New EU data protection regime extends the scope of the European Union data protection laws to all foreign companies processing EU citizens' data. This Regulation provides for the harmonization of data protection rules across the EU, which defines that non-European companies, if they have any personal data on EU citizens in any way, must comply with these regulations.

2. THE MOST IMPORTANT CHANGES INTRODUCED BY THE GDPR REGULATION

The GDPR regulations came into force on 25 May 2018, with the aim of replacing the 1995 Data Protection Directive (Directive 95/46/EC). While Directive 95/46 was in force, EU members adopted local regulations and therefore the laws on the protection of personal data across the EU were not harmonized. By adopting the GDPR, a single legal instrument with direct application has been created in all 28 Member States, and wider, replacing all the different ways in which the previous Directive was implemented. In addition, GDPR also takes into account new technologies that are not covered by the Directive, such as Big Data, mobile applications, social networks, etc. (Babel, 2017)

GDPR introduces new and more comprehensive rules regarding the use and protection of personal data, and the mere fact that penalties for non-compliance with these regulations

reach up to €20 million, or 4% of annual turnover, speaks about the necessity for timely harmonization of business operations with the new regulations.

Figure 1. Important points of GDPR regulation

Some of the key novelties that the GDPR regulation introduces are:

• Citizens' rights

One of the basic ideas for guiding the adoption of GDPR was that citizens can resume control over their data. Thus, companies in possession of personal data, are obliged to inform their users about the ways in which their data is used, to enable them to inspect data, provide copies, or modify incorrect data. One of the novelties is the so-called 'right to be forgotten' (Mantelero, 2013) which means that the existing right to delete data adapts to the reality on the Internet in which our data is constantly published and shared. It is similar to the right to data transferability, which implies that companies dealing with analytics of personal data will have to provide their users, on their request, with all the information about them in machine-readable format, so that this data can be used for others services.

• Records of the processing of personal data

Keeping records of personal data processing, but also formally registering such records with the Commissioner for the Protection of Personal Data is an obligation that is prescribed by the current Law in Serbia. GDPR imposes somewhat fewer obligations, and prescribes only the obligation to keep such records, with the exception of smaller operators

and those that do not collect sensitive data. But here we should wait and see what the new law solutions will be pertaining to these records.

• Privacy by design and Privacy by default (Privacy by design & Privacy by default)

The concepts Privacy by Design and Privacy by Default (Cavoukian, 2011) as a rule will be discussed in detail in future because the implementation of information solutions based on these principles will be an imperative for large systems that handle personal data, but also a business opportunity for software development companies and similar technical solutions.

GDPR prescribes that it is necessary to design data processing and information systems from the very beginning to effectively implement the data protection principles and protect the rights of the persons to whom the data relate to, and that appropriate measures need to be implemented in order to process only data on the personality that are necessary for the specific purpose of processing i.e., to collect minimum data from citizens.

• Reporting security incidents

Despite the fact that investment in infra-red security has increased considerably, we can read almost every day that multi-million personal databases have been often compromised. Accordingly, the GDPR prescribes that in the case of incidents or data compromise (data breach) there is an obligation to notify the competent bodies for personal data protection within 72 hours with the submission of a detailed case report. And not only that, companies that have found themselves in this situation have to inform all persons whose data are compromised.

3. OBLIGATIONS OF THE REPUBLIC OF SERBIA IN ACCORDANCE WITH THE GDPR REGULATIONS

Formal reasons why Serbia must comply with GDPR regulation are the obligations that Serbia has towards the European Union and the obligations that Serbia has imposed on itself. As an EU membership candidate, Serbia is obliged to harmonize its legislation with the EU acquis. According to the Article 81 of the Law on the Confirmation of the Stabilization and Association Agreement between the European Communities and their Member States of the one part and the Republic of Serbia of the other part (SAA, 2013), the Republic of Serbia has committed itself to harmonizing its legislation on the protection of personal data with communitarian legislation and other European and international privacy regulations.

Harmonization with the Regulation implies that not only the applicable Personal Data Protection Act will be changed, but other laws governing the processing of personal data will be amended or adopted. It is also necessary to adopt by-laws. The method of harmonization will also depend on the constitutional order, because the Constitution of the Republic of Serbia determines that the processing of data must be regulated by law.

4. GDPR IMPACT ON THE FUNCTIONING OF THE INFORMATION AND COMMUNICATION SYSTEM OF THE MOI OF THE REPUBLIC OF SERBIA

In the previous period, the Ministry of Interior of the Republic of Serbia has received several complaints from the Commissioner for Information of Public Importance and Personal Data Protection regarding the unauthorized processing of personal data through a video surveillance system and a system for recording radio-communication of police officers (recording of participants in traffic using the so-called 'Interceptor, audio and video surveillance of the conduct of police officers during the performance of duties and tasks within their competences, etc.). (Gligorijević, Jokić & Maksimović, 2016) Consequently, the definition of legal frameworks and drafting of legal norms within the framework of the Law on Records and Processing of Data in the Ministry of Interior of the Republic of Serbia in this area has begun. In this way, for the first time, in a clear, precise and transparent manner, the sphere of personal data processing in the MoI, as well as the data set on the person being processed, and of course the purpose of the processing itself, has been regulated. By adopting the aforementioned Law, which is fully in line with the GDPR regulations and new Law on Police, the area of personal data processing in the Ministry of Interior has been shaped in accordance with current legal requirements.

Since information security means the protection of systems, data and infrastructure in order to preserve the confidentiality, integrity and availability of information, the application of the law affects all citizens, public authorities and businesses that use information and communication technologies. Namely, legal solutions build user trust in the safe functioning of ICT systems, citizens' trust in the protection of personal data in ICT systems, awareness raising about the necessity of implementing information security measures, data protection, protection of ICT systems, security of electronic transactions, efficient mechanisms of protection and realization of rights in the processes of electronic business, electronic data interchange and e-government services.

The Ministry of Interior owns its own information and communication system, which, beside various databases, containing information obtained by the operational work of the MoI members, has also unique national databases with data on citizens of Serbia. (Popović & Maksimović, 2017) These data are crucial in determining the identity of an individual, and any problem, whether it is an inability to access data, unauthorized access, loss or damage to data, can lead not only to the problems for the individual, but also to the moral and material consequences for the MoI, in the sense of losing citizens' confidence in the ability of this ministry to fulfil its competencies, as well as potential damage that might arise from the blocking of certain services provided by the MoI information and communication system. Therefore, the Ministry of Interior already applies comprehensive protection measures in ICT systems and information in general, and thus we have avoided any incidents that could endanger data or degrade the characteristics of the system. Each segment of the system is defended against external influences, and databases are located on a special, internal computer network of the Ministry that has no contact with other networks. In cases when it is necessary to provide access to data to another state

institution, a separate server is formed, separated from the internal network of the Ministry, with a replicated database. (Nedeljković & Forca, 2015)

5. CONCLUSION

The EU General Data Protection Regulation (GDPR) which replaced the Data Protection Directive from 1995, was drafted and designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, to unify personal data processing and to reshape the way organizations across the region approach data privacy. Both organizations that process the EU citizens' data, and those who are not in the European Union, will have to comply with new rules on personal data protection. This practically means that this regulation also applies to the Republic of Serbia, although it is not a member of the EU yet. Accordingly, the Ministry of Interior of the Republic of Serbia has made appropriate changes in its regulations in order to comply with the GDPR regulations. Such an approach encompasses full compatibility in cooperation and exchanging information with all relevant EU institutions.

6. REFERENCES

Babel, C.: *The High Costs of GDPR Compliance,* InformationWeek, UBM Technology Group, 2017.

Blackmer, W.S.: *GDPR: Getting Ready for the New EU General Data Protection Regulation*, Information Law Group, InfoLawGroup LLP, 2016.

Cavoukian, A.: Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers, Information and Privacy Commissioner, Canada, 2011.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 1995.

Gligorijević, M., Jokić, N., Maksimović, A.: Forensic and legal aspects concerning the use of the video surveillance system in proving crimes and offences, Tematski zbornik radova, Dani Arčibalda Rajsa, Tom III, Kriminalističko-policijska akademija, 2016.

Lehavi, A., Larouche, P., Accetto, M., Purtova, N., Yemer, L.: *The Human Right to Privacy and Personal Data Protection: Local-to-Global Governance in the Digital Era*, Research Project Human Rights Working Group, Law Schools Global League, 2016.

Mantelero, A., The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten', Computer Law & Security Review, 2013.

Nedeljković, S., Forca, B.: Evropska strategija bezbednosti i sajber pretnje – značaj za Srbiju, Vojno delo, Ministarstvo odbrane Republike Srbije, 2015.

Popović, R., Maksimović, A.: Institucionalni i pravni okviri upravljanja policijskom organizacijom u sprečavanju i suzbijanju pretnji bezbednosti informaciono-komunikacionog sistema Ministarstva unutrašnjih poslova, Upravljanje

policijskom organizacijom u sprečavanju i suzbijanju pretnji bezbednosti u Republici Srbiji, Tematski zbornik radova, Kriminalističko-policijska akademija, 2017.

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), Brussels, 2016.

Stabilisation and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Serbia, of the other part, Brussels, 2013.