THE EUROPEAN JOURNAL OF APPLIED ECONOMICS

EJAE 2022, 19(1): 55 - 65
ISSN 2406-2588
UDK: 342.738(4-672EU)
342.727(4-672EU)
004.056.5:34(4-672EU)
DOI: 10.5937/EJAE19-36596
**Original paper/Originalni naučni rad**

# GDPR AND CHALLENGES OF PERSONAL DATA PROTECTION

**Žaklina Spalević*, Kosana Vićentijević**

Singidunum University,
Belgrade, Serbia

**Abstract:**
This paper discusses the challenges of implementing GDPR regulation in the EU and the Republic of Serbia. The regulations governing the issue of personal data protection are outlined. Emphasis is placed on reconciling this issue in the Republic of Serbia with EU legislation. The aim of this paper is to look at GDPR regulations from several standpoints of the business of taxpayers. It is necessary to include all segments of a business entity in the implementation of this regulation, as well as bodies at the national level. It is necessary to adopt by-laws in order to fully implement the Law on Personal Data Protection in the Republic of Serbia.

**Article info:**
Received: February 22, 2022
Correction: February 24, 2022
Accepted: March 17, 2022

**Keywords:**
GDPR,
personal data,
compliance,
data protection.

## INTRODUCTION

Personal data protection mechanisms have changed during the development of society. The area of personal data protection at European level was last regulated in 1995. Viewed from the perspective of technological and social development, the daily activities of people on a large scale have changed under the influence of information and communication technologies. Information and communication technologies have enabled networking, centralization of data and the availability of data online. Viewed from the perspective of local governments and the government sector, almost every sector has been digitized since the last regulation of personal data protection. This practically means that all personal information about citizens is stored digitally either on a local newsletter or centralized and can be accessed from anywhere (Pannadai, 2019). Furthermore, from the perspective of a personal user, the expansion of web services in the domain of communication, social networks, electronic payments, electronic bookings, electronic wallets has led to the exchange of a large amount of information containing personal data of users of such services. For example, Facebook is one of a number of popular social networks used on a daily basis with 1.3 billion users, which leads to a huge daily exchange of information.

*E-mail: zspalevic@singidunum.ac.rs

If we add to this other social networks, as well as the information of telecommunication operators about communication of their users, data collected through cookies, existence of Big Date etc., it is clear that personal data is treated as a trading resource. This practically means that whoever owns the personal data of the inhabitants of the planet has a kind of domination as well (Rašić, 2017).

A step forward in the protection of personal data was the introduction of General Data Protection Regulation (GDPR), adopted in 2016. However, this regulation came into force in 2018, and the delay in its implementation was due to the need for adaptation and adaptation. After an adjustment period, Veritas tested the degree of adaptation success. Based on the survey, only 2% of the respondents fully adapted their way of doing business to GDPR, although 31% said they had fully implemented EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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) as of May 25, 2018. The GDPR regulation deserves special attention: legal, economic, digital, accounting, auditing and other aspects of the digital business environment. GDPR gives the EU residents control over their personal data, wherever their data is located in the world. Not only does the GDPR standardize regulations across the EU and the European Economic Area, it also affects all businesses that process data from the EU countries (Daigle & Khan, 2020). All EU companies are subject to GDPR. Given the global scope of today's digitalisation and e-commerce, the impact of GDPR will surely be tracked and the regulation will be implemented by companies around the world, located beyond the EU's borders. GDPR replaces Data Protection Directive 95/46 / EC and is designed to:

- harmonize personal data privacy laws across the EU,
- protect and empower all EU citizens with regard to data privacy,
- reshape the way organizations across the region access data privacy.

GDPR represents the most important change in data privacy regulation in the last 20 years. As such, it is fundamentally reshaping the way personal data is processed in every sector, from healthcare to banking and beyond, not only in the EU, but around the world, depending on what data is processed and where it is processed. The importance of the right to the protection of personal data (in relation to health) is also underlined by the case law of the European Court of Human Rights and the EU Court of Justice (Bevanda & Čolaković, 2016). GPDR basically requires both individuals and organizations and institutions that collect and process personal data to properly list, categorize and code the data. In this way, the information about users that is considered personal, as well as any combination of facts that can be used to identify an individual must be adequately treated. The implementation of GDPR provides individuals with greater control over their personal data and imposes many obligations on companies that collect and analyze personal data. Personal data means any information that can be used to identify an individual accurately, including but not limited to: name, Unique Master Citizen Number, location data, physical, physiological, genetic, mental, economic, social, cultural or any other factor (Badovinac, 2018).

Compliance with GDPR is binding on all businesses. It is therefore vital for businesses to be able to provide evidence of their internal framework and transparency regarding their data processing practices, with data collection, utilization, storage and erasure across the data management lifecycle (He & Wu, 2019). Over the years, businesses have invested in control frameworks to increase compliance with data protection. Business applications that exist outside these frameworks can compromise the overall security and compliance of the entity.

It is for these reasons that GDPR requires the revision of business models in companies that offer their goods and services to EU residents. Companies that collect personal data before processing must obtain the consent of individuals for their use and it is necessary that individuals be informed of the purpose of collecting their personal data.

Serbia has been waiting for a long time to pass a new Law on Personal Data Protection, which would incorporate GDPR principles into the domestic legal framework and align this area with EU standards. This is crucial for the adequate exercise of citizens' rights and the development of domestic companies using personal information in their business, because this is the only way to ensure legal certainty. The Ministry of Justice task force tasked with drafting the new law was formed back in 2013, but following one unsuccessful attempt from 2015 until 2018, it failed to prepare a normative solution that would be in line with the European regulation (Hoofnagle, *et al*., 2019). However, due to the need for compliance with EU law and standards for the protection of personal data, the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia", No. 87/2018) was adopted in the Republic of Serbia due to the need for new solutions and elimination of the deficiencies of the current law. This law was adopted in November 2018, and came into effect on August 21, 2019.

The authors have presented the topic of their paper clearly, indicating its scope and presenting the objectives and organization of the paper. The novelty of the research presented in the paper should be emphasized and the subject well documented in the up-to-date literature (Starchon & Pikulik, 2019).

## GDPR IN AN INTERNATIONAL ENVIRONMENT

The protection of personal data is subject to the legal provisions of the People's Republic of China. In June 2017, China introduced a law that bridges the gap between cyber security and personal data protection. This law is actually the average set of provisions of the EU Network and Information Systems (NIS) Directives and GDPR. In many aspects, the Cybersecurity Law of the People's Republic of China (CSL) complies with the GDPR – for example, requiring consent to collect data and protect against code loss (Brodin, 2019). CSL also prescribes other important considerations for multinationals as "critical" categories, such as utilities and banks, that store personal data collected in China (domestically), which may require repatriation of data from overseas Cloud services. In addition, companies must undergo a review by the regulatory body to transfer large amounts of personal data abroad. Any business entity in China may be exposed to the risk of compliance with CSL regulations . Legal and IT teams are already working to comply with GDPR regulations, and the internal audit is in a position to provide security for conducting top-down risk assessments (Voigt, P., & Bussche, 2017). In this process, internal auditors consider how likely it is that a businesses will comply by using a technology gap analysis to review the existing controls and identify key areas that need improvement, and consult with them about the practical implementation of new controls and processes in GDPR implementation. The following are some key issues when implementing and monitoring GDPR compliance:

- whether a risk assessment has been carried out to understand if the economic component is GDPR compliant and where further compliance work is required,
- whether the business entity has mapped the database of personal data (as opposed to asset data),
- whether the business entity's cyber parameters are secure and encrypted,
- whether the business entity processes personal data on a large scale and whether an internal Data Protection Officer (DPO) is qualified to protect the data,

- whether there is a reporting procedure for the relevant national authorities for misuse of personal data,
- whether the business entity has established an awareness program and training of employees in the management, security and disclosure of personal data,
- whether data protection principles are incorporated into contracts with relevant third parties.

GDPR has certain requirements regarding the transfer of personal data outside the EU. One is that data can be transferred to countries deemed to have adequate legal safeguards. Currently, the USA has weak personal data protection laws and does not meet this requirement (George, *et al.,* 2019), though a program known as the EU-US Privacy Shield certified that companies from the US have the appropriate controls to receive personal information from EU businesses. However, a group of MEPs called off this possibility, arguing that it was not an adequate safeguard mechanism and should be implemented when the weaknesses in the program are fully taken care of. European companies therefore need to keep an eye on the development of their US partners (Greze, 2019).

An example of GDPR application is large IT companies that have aligned their software solutions with GDPR. SAP has assessed the need to implement new procedures in its SAP SuccessFactors HCM Suite (Finck & Pallas, 2020). SAP has taken into account that in order to comply with GDPR, it will need to specifically record the personal data of employees. In doing so, the personal data domain at SAP included basic personal information as well as bank accounts, human resources data, employee qualifications, education details, salary levels and social security data. Also, records are kept of all details about access to the system by the employees, as well as all the authority in the system. The package created in this way is set up in SAP Cloud, where data security is ensured by encrypting them. Another example of implementing GDPR is visible in Oracle. Oracle noted that GDPR rigor would require the coordination of many entities such as legal and human resources, marketing, security and IT. Many IT infrastructure domains also need to be analyzed to find personal information, such as: structured data, different types of files, MAC or IP addresses and metadata. Oracle's announcements are also aimed at improving security controls (Roote & Chakravaty, 2018). Only 27% of businesses in the EU are GDPR compliant after the date indicated as mandatory (25/05/2018). At the end of 2018, compliance rates are estimated at 93%, 74% of respondents pointed out, according to a TrustArc survey (Gulczynska, 2021). GDPR also takes into account new technologies not covered by the Directive such as Big Data, mobile applications, social networks, etc.

In the Republic of Croatia, on the basis of the competences established by the Law on Implementation of the General Data Protection Regulation ("Official Gazette", no. 42/18), the Agency for Personal Data Protection was established to ensure the implementation of EU Regulation 2016/679. The Agency acts independently of the executive and legislative branches, not receiving instructions and orders from any state body. The independence of the Agency is enshrined in the Convention on the Protection of Individuals with regard to Automatic Data Processing (Council of Europe Convention 108 ) and the Additional Protocol to the Convention for the Protection of Personal Data pertaining to the automatic processing of personal data concerning supervisory authorities and the international exchange of data (Starcevic, K., *et al.*, 2018). The main tasks of the Agency are to act effectively in fulfilling all rights and obligations in the field of personal data protection imposed on the Republic of Croatia as a member of the EU and the Council of Europe, increasing the responsibility of all participants in the process of processing personal data related to the application of the regulations covered by the legal framework for personal data protection in the Republic of Croatia, alongside appropriate implementation of information security measures.

## CONTRIBUTION OF EU REGULATION 2016/679 (GDPR) TO THE PROTECTION OF PERSONAL DATA

Data processing, especially personal data, new IT tools and the digital market have increased the need for better privacy protection of new digital products and services. The solution is set out in a new reform of the EU framework for the protection of personal data, which changes the ways in which personal data is managed and implemented at the same time in all organizations that have personal data of EU citizens (Voss & Houser, 2019). The EU General Data Protection Regulation 2016/679 has been in force since 25 May 2018. GDPR has significantly changed the rules that define personal data, introducing new concepts and compliance, planning, implementation, maintenance compliance, and risk assessment. The key premise of the development of the modern digital economy is based on the accelerated development of information and communication technologies, while responding to new challenges and threats to privacy and protection of personal data (Čizmić & Boban, 2018). Today, 250 million people use the internet in the EU (Burri & Schar, 2016). More and more personal information is online, whether it is online banking, shopping, social networks or electronic tax refunds. Individuals have the right to the protection and storage of personal data. There are a number of potential risks: unauthorized disclosure, identity theft, or cyberbullying (Chambers & Barger-Walliser, 2021).

Compared to the previous regulation (Data Protection Directive), the importance of applying the principles is more pronounced, the definitions are clearer, and at the same time extended by certain, modern principles of personal data protection (Weber, *et al*., 2020). Unlike the previous Directive, where the principles were primarily concerned with data quality, the Regulation binds the principles to the processing of personal data. The principles of the Regulation, which are also covered by the previous regulation, are as follows: the principle of legality, fair processing and transparency, the principle of purpose limitation, the principle of minimum data processing, the principle of accuracy, the principle of limitation of data storage (Yu, 2021). However, the principle of integrity and confidentiality is an integral part of the Regulation and covers the protection of data by technical and organizational measures, informing the supervisory authority and persons to whom the data belong in case of a data breach. However, probably the most important principle is the principle of responsibility, which introduces the obligation of the operator to prove that they comply with all principles. Only those taxpayers who can successfully prove compliance will avoid liability for any irregularities in the application of regulations (Mraznica, 2017). The protection of personal data is a fundamental right of every individual in the EU. The entry into force of Regulation 2016/679 allows for the control of personal data and the improvement of security on the Internet and in other databases (Casagran & Vermeulen, 2021).

New EU individuals' rights resulting from GDPR include:

- the right to receive clear and comprehensible information about who processes personal data, what data is processed and why it is processed (article 12-14 GDPR),
- the right of access to personal data held by a business entity about an individual (article 15 GDPR),
- the right to require the natural person to transfer all personal data to another provider (article 20 GDPR),
- the right to "delete" – an individual may request the deletion of personal data if he / she does not want to be further processed and the business entity does not have a justified reason to hold them (article 17 GDPR),
- when a business operator seeks the consent of an individual for data processing, it must clearly state this (article 4. paragraph 11. and article 7 GDPR),

- articles 33 i 34 GDPR regulate the situation of theft or loss of personal data, stipulating that the business entity must notify the individual and the appropriate data protection supervisory authority, and that the business entity that does not do so may be fined,
- article 8 GDPR regulates better protection of children online, and others.

The GDPR rules of May 2018 include improving the resolution of the implementation of personal data protection in several aspects: clarity, user consent, greater transparency, greater rights, stronger implementation (Table 1).

**Table 1**. A new era of data protection in the EU

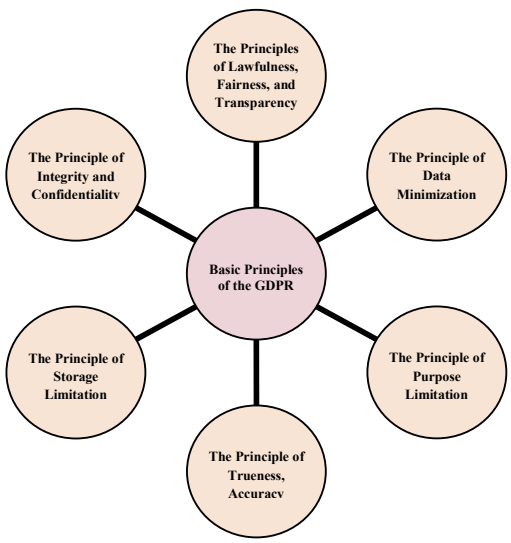
| Prior to the implementation of EU Regulation 2016/679 | With the entry into force of EU Regulation 2016/679 |
|---|---|
| **CLEAR LANGUAGE** | |
| Often businesses explain their privacy policies in lenghty and complicated terms. | Privacy policies will have to be written in a clear, straightforward language. |
| **CONSENT FROM USER** | |
| Businesses sometimes assume that the user's silence means consent to data processing, or they hide a request for consent in long, legalistic, terms and conditions — that nobody reads. | The user will need to give an affirmative consentbefore his/her data can be used by a business. Silence is no consent. |
| **MORE TRANSPARENCY** | |
| The user might not be informed when his/her data is transferred outside the EU | Businesses will need to clearly inform the user about such transfers. |
| Sometimes businesses collect and process personal data for different purposes than for the reason initially announced without informing the user about it. | Businesses will be able to collect and process data only for a well-defined purpose. They will have to inform the user about new purposes for processing. |
| Businesses use algorithms to make decisions about the user based on his/her personal data (e.g. when applying for a loan); the user is often unaware about this. | Businesses will have to inform the user whether the decision is automated and give him/her a possibility to contest it. |
| **STRONGER RIGHTS** | |
| Often businesses do not inform users when there is a data breach, for instance when the data is stolen. | Businesses will have to inform users without delay in case of harmful data breach. |
| Often the user cannot take his/her data from a business and move it to another competing service. | The user will be able to move his/her data, for instance to another social media platform. |
| It can be difficult for the user to get a copy of the data businesses keep about him/her. | The user will have the right to access and get a copy of his/her data, a business has on him/her. |
| It may be difficult for a user to have his/her data deleted. | Users will have a clearly defined "right to be forgotten" (right to erasure), with clear safeguards. |
| **STRONGER ENFORCEMENT** | |
| Data protection authorities have limited means and powers to cooperate. | The European Data Protection Board grouping all 28 data protection authorities, will have the powers to provide guidance and interpretationand adopt binding decisions in case several EU countries are concerned by the same case. |
| Authorities have no or limited fines at their disposal in case a business violates the rules. | The 28 data protection authorities will have harmonised powers and will be able to impose fines to businesses up to 20 million EUR or 4% of a company's worldwide turnover. |

*Source:* Adapted from https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_hr.pdf

## IMPLEMENTATION OF GDPR IN THE REPUBLIC OF SERBIA

The irreversable trend of the technology integration improves the quality of communications, refines the development of technologies, but also has an important task in establishing models of data protection, especially personal ones (Wrigley, 2021). The key objective of EU data protection law reform is to protect the most valuable part of the individual and the concept of individuality as opposed to universality. The first Personal Data Protection Act („Official Gazette of the Republic of Serbia", no. 97/2008, 104/2009 (the second law), 68/2012- Decision of the Constitutional court and 107/2012) in the Republic of Serbia was enacted in 2008. Due to compliance with EU regulations on personal data protection, a new Law on Personal Data Protection was adopted in 2018 in the Republic of Serbia (Presthus & Sonslien, 2020). Personal Data Protection Act („Official Gazette of the Repblic of Serbia", no. 87/2018) should ensure respect for the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, establish a clear legal framework in the field of personal data protection in the Republic of Serbia, regulate the processing of personal data, rights, obligations and responsibilities of data controllers, the data processor and all recipients of data, as well as the jurisdiction and position of an independent authority for the protection of personal data. This Law was only a basic regulation, and it was necessary to harmonize it with a whole series of legal acts and by-laws within nine months from the day the Law entered into force. (21/11/2018). Businesses also needed time to prepare and adapt to the implementation of the Law on Personal Data Protection. The Law incorporates the basic principles of GDPR through Article 5 (Figure 1).

**Figure 1.** Basic principles of GDPR




This Law (Article 2) provides protection of the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. According to Article 4, paragraph 1. Item 1) "personal data" means any information relating to an individual whose identity is determined or identifiable, directly or indirectly, especially based on an identity mark, such as name and identification number, data location, an identifier in electronic communications networks, or one or more features of his physical, physiological, genetic, mental, economic, cultural and social identity (Rademacher, 2020).

"Processing of personal data" in Article 2, Paragraph 1, Item 3), is defined as any activity or set of actions performed automatically or non-automated with personal data or their sets, such as collecting, recording, sorting, grouping , that is, structuring, storing, depicting or modifying, disclosing, seeing, using, detecting by transmitting or delivering, duplicating, expanding or otherwise making available, comparing, limiting, deleting or destroying (Hubig, 2020).

One of the main goals of GDPR is to further strengthen the rights to the protection of personal data, that is to say, to give individuals greater control over their personal data. Fines are provided for all offenses specified in the Act (Krivokapic, *et al.,* 2019). The infringements may be commited by the operators, processors having legal capacity, entrepreneurs, natural persons, responsible legal persons, state bodies, territorial autonomy bodies, local self-government units, responsible persons in representative offices or business units and foreign legal entities (Andonovic, & Prlja, 2020). When it comes to sanctions imposed on those who violate of the provisions of this law, the regulation significantly tightened the regime of administrative fines in case of non-compliance with obligations. The degree of punishment is defined depending on the type of offense. For example, fines can be imposed up to € 10 million. In the case of companies, the penalty may be imposed up to 2% of the total annual worldwide turnover for the previous financial year (Gligorijević, M., Popović, R., & Maksimović, 2018).

The fines defined in this way can be imposed in the case of irregularities recorded in the domain of technical, organizational capacity as well as inaccuracies in the field of record keeping, impact assessment and the appointment of persons. In case of violation of basic processing principles, rights of persons, data transfer, non-compliance with the order of the supervising regulator, a fine of up to 20 million euros can be imposed; if a company is involved, the amount of the penalty may go up to 4% of the total annual turnover worldwide for the previous financial year (Klar, 2020). In addition to the monetary regulations, the regulation also prescribes other types of sanctions that give the supervisory regulatory body additional powers. For example, the regulatory body has at its disposal appropriate measures that can range from corrective measures and the operator's compliance with the prescribed obligations to the possibility of prohibiting the use of personal data. The prohibition on the processing of personal data may include further processing, transfer, orders for deletion of data, corrections, and even withdrawal of quality certificates.

## CONCLUSIONS

Digitization and new ways of processing personal data have prompted the adoption of a new instrument that will protect the rights and personal freedoms of individuals regarding the processing of their personal data. The EU Data Protection Regulation 2016/679 or GDPR represents an advance in the field of personal data protection. The impact of GDPR is primarily seen in the fact that its adoption ensures a uniform treatment of data protection supervisory authorities, leading to a simpler and more equal protection of the rights of all individuals in the EU. New definitions and simplified existing ones define biometric and genetic data, more accurately describe existing concepts, strengthen the rights of respondents and reduce and simplify certain administrative obligations of personal data controllers, strengthen supervision and the possibility of imposing penalties on bodies responsible for personal data protection.

In this paper we have presented some of the main challenges before the implementation of the Law on Personal Data Protection in the Republic of Serbia.

The study of GDPR application in this paper can serve as a continuation of research on this topic, for different views of this topic from the aspect of internal audit, external audit, accounting, IT sector, and other activities involved in the implementation and supervision of this regulation.

## REFERENCES

Andonovic, S., & Prlja, D. (2020). *Osnovi prava zastite podataka o licnosti*. Beograd: Institut za uporedno pravo. Retrieved January 29, 2022, from http://iup.rs/wp-content/uploads/2020/09/2020-Andonovic-Prlja-Osnovi-prava-zastite-podataka-o-licnosti.pdf

Badovinac, N. (2018). Osvrt na GDPR uredbu i sugestije za razvoj aplikativne podrške, *Info M, 17(65)*, 11-16. Retrieved December 11, 2021, from https://infom.fon.bg.ac.rs/index.php/infom/article/view/2271/2243

Bevanda, M., & Čolaković, M. (2016). Pravni okvir za zaštitu osobnih podataka (u vezi sa zdravljem) u pravu Evropske Unije, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 37(1)*, 125-154. https://doi.org/10.30925/zpfsr.37.1.5

Brodin, M. (2019). A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research, 4*, 243-264. https://doi.org/10.1007/s41125-019-00042-z

Burri, M., & Schar, R. (2016). The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy, 6,* 479-511. https://doi.org/10.5325/jinfopoli.6.2016.0479

Casagran, C., & Vermeulen, M., (2021). Reflections on the murky legal practices of political micro- targeting from a GDPR perspective. *International Data Privacy Law, 11(4)*, 402. https://doi.org/10.1093/idpl/ipab018

Cizmic J., & Boban M., (2018), Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 39(1)*, 377-410. https://doi.org/10.30925/zpfsr.39.1.13

Chambers, R., & Barger-Walliser, G. (2021). The Future of International Corporate Human Rights Litigation: A Transatlantic Comparison. *American Business Law Journal. 58(3)*, 579-642. https://doi.org/10.1111/ablj.12193

Daigle, B., & Khan M. (2020). The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities. *United States International Trade Commission Journal of International Commerce and Economics. 1-38*. https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf

Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law, 10(1)*, 11–36. https://doi.org/10.1093/idpl/ipz026

Foote, P., & Chakravarty, S. (2018). EU GDPR biometric compliance systems, Retrieved January 23, 2021, from https://biometri-cupdate.com/201803/eu-gdpr-biometric-compliance-systems

George. D., Reutimann, K., & Larrieux, A. (2019). GDPR bypass by design? Transient processing of data under the GDPR. *International Data Privacy Law. 9(4)*, 285-298. http://dx.doi.org/10.2139/ssrn.3243389

Gligorijević, M., Popović, R., & Maksimović, A. (2018). 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. In Stanarevic, S., Mandic, G. & Katic, Lj. (Eds.) *4th International Conference on Human Security: the Proceedings of Human Security and New Technologies* (pp. 75-81). Belgrade: Faculty od Security Science. https://doi.org/10.18485/fb_ic4hs.2018.8

Greze, B. (2019). The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives. *International Data Privacy Law, 9(2)*, 109–128. https://doi.org/10.1093/idpl/ipz003

Gulczynska, Z. (2021). A certain standard of protection for international transfers of personal data under the GDPR. *International Data Privacy Law, 11(4)*, 360–374. https://doi-org.eres.qnl.qa/ 10.1093/idpl/ipab013

He, L., Lu, Y., & Wu, He. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management. 22(1)*, 1-6. https://doi.org/10.1080/1097198X.2019.1569186

Hoofnagle, C., Sloot, B., & Borgesius Frederik. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law. 28(1)*, 65-98. https://doi.org/10.1080/13600834.2019.1573501

Hubig, C. (2020). Benefits and Limits of Autonomous Systems in Public Security. *European Journal for Security Research. 5*, 25–37. https://doi.org/10.1007/s41125-019-00057-6

Klar, M. (2020). Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies. *Hastings science technology law journal. 11(2)*, 101-154. Retrieved December 17, 2021 from https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1095&context= hastings_science_technology_law_journal

Krivokapić, D., Adamović, J., Tasić, D., Petrovski, A., Kalezić, P., & Krivokapić, Dj. (2019). *Vodic kroz zakon o zastiti podataka o licnosti GDPR – tumačenje novog pravnog okvira*. Misija OEBS-a u Srbiji SHARE fondacija. Retrieved December 17, 2021 from https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf

Mraznica, E. (2017). GDPR – Novi izazov zaštite podataka o ličnosti. *Bankarstvo, 47(4)*, 166-177. Retrieved November 17, 2021. from https://scindeks-clanci.ceon.rs/data/pdf/1451-4354/2017/1451-43541704166M.pdf

Pannagai, P. (2019). GDPR: A Privacy Regime. *International Journal od Trend in Scientific Research and Development. 3(4)*, 713-716. https://doi.org/10.31142/ijtsrd23460

Presthus, W., & Sonslien, K. (2020). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management, 9(1)*, 38-53. https://doi.org/10.12821/ijispm090102

Rademacher, T. (2020). Of New Technologies and Old Laws: Do We Need a Right to Violate the Law? *European Journal for Security Research. 5*, 39–58. https://doi.org/10.1007/s41125-019-00064-7

Rašić, M. (2017). Šta je to GDPR i zašto se tiče i srpskih kompanija koje posluju sa ličnim podacima? Retrieved November 29, 2021. from https://www.netokracija.rs/gdpr-definicija-uredba-136384

Starčević, K., Glavas, J., & Crnkovic, B. (2018). Implementation of the general data protection regulation in companies in the republic of Croatia. *Ekonomski Vjesnik, 31(1)*, 163-176. Retrieved November 15, 2021. from https://hrcak.srce.hr/202007

Starchon, P., & Pikulik, T. (2019). GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones. *Procedia Computer Science. 151*. 303-312. https://doi.org/10.1016/j.procs.2019.04.043

Vanberg, A., & Unver M. (2017). The right to data portability in the GDPR and EU competition law : odd couple or dynamic duo? *European Journal of Law and Technology, 8(1)*. Retrieved November 8, 2021. from https://ejlt.org/index.php/ejlt/article/view/546/727

Voigt, P., & Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Cham, Switzerland: Springer International Publishing AG.

Voss, G., & Houser, K. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal. 56(2)*, 287-344. https://doi.org/10.1111/ablj.12139

Weber, P., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research, 20*, 565–587. https://doi.org/10.1007/s10660-020-09422-3

Wrigley, S., (2021). B v Latvijas Republikas Saeima: GDPR Limits Publishing of Information about Drivers Who Receive Penalty Points. *European Data Protection Law Review, 7(4)*. 609-613. https://doi.org/10.21552/edpl/2021/4/18

Yu, X., (2021). The three legal dimensions of China's big data governance. *Journal of Chinese Governance*. https://doi.org/10.1080/23812346.2021.1988267

# GDPR I IZAZOVI U VEZI SA ZAŠTITOM LIČNIH PODATAKA

**Rezime:**

U radu se razmatraju izazovi implementacije GDPR regulative u EU i Republici Srbiji. Navedeni su propisi koji uređuju pitanje zaštite podataka o ličnosti. Akcenat je stavljen na usklađivanje ovog pitanja u Republici Srbiji sa zakonodavstvom EU. Cilj ovog rada je da sagleda GDPR propise sa više stanovišta poslovanja poreskih obveznika. U sprovođenje ovog propisa neophodno je uključiti sve segmente privrednog subjekta, kao i organe na nacionalnom nivou. Neophodno je doneti podzakonska akta kako bi se Zakon o zaštiti podataka o ličnosti u Republici Srbiji u potpunosti primenio.

**Ključne reči:**

GDPR,
lični podaci,
usklađenost,
zaštita podataka.