Универзитет у Новом Саду
Правни факултет у Новом Саду

Szegedi Tudományegyetem
Állam- és Jogtudományi Kar

Хармонизација српског и мађарског права са правом Европске уније

A szerb és a magyar jog harmonizációja az Európai Unió jogával

Harmonisation of Serbian and Hungarian Law with the European Union Law

Тематски зборник

Tematikus tanulmánykötet

Thematic Collection of Papers

Књига VI

VI. Kötet

Volume VI

Правни факултет у Новом Саду, Центар за издавачку делатност,
Нови Сад, 2018

Újvidéki Jogtudományi Kar, Kiadói Központ, Újvidék, 2018

Faculty of Law Novi Sad, Publishing Center, Novi Sad 2018.

УНИВЕРЗИТЕТ У НОВОМ САДУ
ПРАВНИ ФАКУЛТЕТ
ЦЕНТАР ЗА ИЗДАВАЧКУ ДЕЛАТНОСТ
Трг Доситеја Обрадовића 1
21000 Нови Сад
www.pf.uns.ac.rs

ХАРМОНИЗАЦИЈА СРПСКОГ И МАЂАРСКОГ ПРАВА СА ПРАВОМ ЕВРОПСКЕ УНИЈЕ

За издавача:
Проф. др Бранислав Ристивојевић, декан Правног факултета у Новом Саду
Проф. др Љубомир Стајић, управник Центра за издавачку делатност
Мр Радмила Дабановић, главни и одговорни уредник монографских издања

Рецензенти:
Prof. Dr. Gellén Klára
Prof. Dr. Blutman László
Prof. Dr. Pap András
Doc. Dr. Mezei Péter
Проф. др Драган Милков
Проф. др Ранко Кеча
Проф. др Владимир Марјански
Доц. др Атила Дудаш

Технички уредници:
Др Лука Батуран, асистент са докторатом
Милица Ковачевић, асистент

Идејно решење корица
Милан Левнајић

Компјутерска обрада текста
Владимир Ватић, ГРАФИТ, Петроварадин

Штампа
„Футура", Петроварадин

Тираж
60 примерака

ISBN 978-86-7774-213-3

Објављивање ове публикације одобрио је Издавачки савет Центра за издавачку делатност Правног факултета у Новом Саду на седници одржаној 8. марта 2018. године.

САДРЖАЈ

TARTALOMJEGYZÉK

TABLE OF CONTENTS

Оригинални научни рад 347.181:342.7:[061.1EU

Szilvia Váradi, Ph. D., Assistant Professor
University of Szeged
Faculty of Law
varadiszilvia@juris.u-szeged.hu

THE EFFECTS OF GDPR ON PUBLIC ADMINISTRATION

Abstract: *The General Data Protection Regulation (GDPR) of the European Union entered into force after a two-year period on 25th May 2018, and since then it has a high impact not only on private-, but public sector organisations. The GDPR introduces many significant changes and restrictions regarding the activities of public authorities and bodies. This new regulation empowers the data subject to control the use of their own personal data, and while the consent of the data subject (user of a service) is one of the basic legal grounds to process personal data, there are a lot of exceptions for the public sector, such as the so-called right to be forgotten, data portability, data protection impact assessment, etc. The aim of this paper is to explore these special provisions and analyse them to clarify the uncertainty still existing in this field.*

Key words: *GDPR, European Union, personal data protection, public authorities and bodies, public sector.*

The European Union has performed the reform of the European data protection rules, which resulted in the General Data Protection Regulation (GDPR)[1] entered into force after a two-year period on 25th May 2018. Since that time, several papers addressed its general aspects and the main impacts, however there are only few ones describing specific impacts of the GDPR on the public sector. Almost a year in force has passed, and there is still some uncertainty, how we can apply these rules. As a result, in this paper we analyse the relevant provisions of GDPR affecting the public sector.

[1] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

As it has the legal form of a regulation, the GDPR automatically formed a part of the domestic legal order of each Member State of the European Union (EU), and it required no further transposition. According to the direct application principle, it is normally illegal for a Member State to adopt an implementing legislation, because such norms might contain changes, which acts against the uniform application of the regulation.[2] In case of the GDPR, it requires national authorities to adopt implementing measures to specify some provisions. However, if there is such a requirement, a failure to implement the regulation will be a breach of EU law.[3]

Public sector: public authority or body

Public sector organizations collect and hold vast amounts of data, much of which has a sensitive nature. Therefore, the scope of GDPR also holds for that sector. The Article 4 (7) of GDPR contains that a 'controller' can also be a public authority, agency or other body, which alone or jointly with others determines the purposes and means of the processing of personal data. The Article 4 (8) of GDPR clarifies that a 'processor' can be among others public authority, agency or other body, which processes personal data on behalf of the controller.

Nevertheless, in GDPR we cannot find any definition for the term 'public sector', and it also does not contain what constitutes a 'public authority or body'. According to the Article 29 Working Party (Art. 29 WP)[4], such a notion is to be determined under the national law. Public authorities and bodies include national, regional and local authorities, but they, under the applicable national laws, typically also include a range of other bodies governed by public law. However, a public task may be carried out, and public authority may be exercised not only by public authorities or bodies, but also by other natural or legal persons governed by public or private law, in sectors such as public transport services, water and energy supply, road infrastructure, public service broadcasting, etc.[5] These cases are very similar to when the personal data of the data subject are processed by a public authority or body.

Public authorities that collect data in the framework of a particular investigation, in accordance with a legal obligation for the exercise of their official mission, are not seen as recipients and thus do not have to comply to GDPR.[6] The

[2] Chalmers 2010, 99. p.

[3] C-128/78 Commission vs. United Kingdom, Tachographs. Judgment 1978] 425. p. ECLI:EU:C:1979:32.

[4] The Article 29 Working Party (Art. 29 WP) was set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, having regard to Articles 29 and 30 thereof. It was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018. Since then it was ceased to exist and has been replaced by the European Data Protection Board (EDPB).

[5] Art. 29 WP: Guidelines on Data Protection Officers ('DPOs'). 16/EN WP 243. Adopted on 13 December 2016. 6. p.

[6] GDPR, Article 2 and Article 9.

expression 'particular' indicates that this is only valid in the context of an inquiry into a specific situation. The GDPR contains different examples, such as inquiries by tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities.[7]

Competent authorities, mainly police and judicial services, are also excluded "for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".[8] The GDPR also provides a legal basis for "processing of personal data relating to criminal convictions and offences or related security measures [...]. Any comprehensive register of criminal convictions shall be kept only under the control of official authority".[9] This means that the entire parts of police and judicial activities related to the prevention and prosecution of crimes are out of the material scope of the GDPR, because of the special rules affecting them.[10]

Another exception is when Member States carrying out activities which fall within the scope of the EU Common Foreign and Security Policy.[11] This provision broadly covers data processing by services and departments related to ministries of Foreign Affairs. It has also to be noted that these services shall demonstrate that the processing of personal data is based on the EU Common Foreign and Security Policy. Thereby to the specific areas of public sector activities, broadly related to oversight, crime detection and crime prevention the GDPR is not applicable. These situations should be clarified before processing personal data and distinguished from the more common processing by public authorities, where GDPR fully applies.

Personal data

Personal data means any information relating to an identified or identifiable natural person, the so called 'data subject' in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[12]

---

[7] GDPR Recital (31).

[8] GDPR, Article 2, 2 (d).

[9] GDPR Article 10.

[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, OJ L 119, 4.5.2016, 89–131. pp.

[11] GDPR, Article 2, 2 (b).

[12] GDPR Article 4 (1).

Some types of personal data are considered off-limits for processing, namely "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".[13] Some other exceptions are such as: in the framework of legal obligations of the data controller considering employment, social security and social protection law;[14] for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.[15]

Principles relating to data processing

The governing principle of the GDPR is 'purpose limitation' meaning that personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[16] Other important requirement is the 'data minimisation' which means that the personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[17] Public sector bodies, however, can retain data if there is a public interest rationale for doing so, even if individuals have requested it be removed.

Additionally the 'accuracy' principle contains that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[18] A common problem which is also relevant to the private sector, is the relevance of the data they hold. Often data bases and filing systems are overloaded with mass amounts of outdated and unnecessary information. Organizations need to challenge themselves to identify what the data they hold is for, using the GDPR as an opportunity to clear the backlog.

It has a high importance that personal data shall be processed lawfully, fairly and in a transparent manner. To achieve this goal, Article 6 of the GDPR strictly describes what constitutes lawful processing of personal data. From these legal bases we point out only the relevant situations regarding public authorities.

Consent is one of the legal grounds for processing with restrictions for the public sector.[19] As part of the stricter requirements, consent must be explicit, and

[13] GDPR Article 9, 1.
[14] GDPR Article 9, 2 (b).
[15] GDPR Article 9, 1 (i).
[16] GDPR Article 5, 1. (b).
[17] GDPR Article 5, 1. (c).
[18] GDPR Article 5, 1. (d).
[19] GDPR Article 6, 1. (a).

permissions must be easily understood with the minimum use of jargon. The regulation empowers individuals with control over their own personal data whilst also making organizations who deal with personal information more accountable for its security. The GDPR does allow a data transfer based on consent of the data subject, however, public sector organizations can hardly ever use this exemption. The rationale behind this is the relational imbalance between the government and its citizens, which is impeding with the requirement that consent must be 'freely given'.[20] The consent given by the data subject to process personal data has major role in the field of private sector. Public authorities, however, don't have to comply with this in so far as processing data to fulfil a task which is in the public interest.

In case of public sector, the following bases could be used: processing is necessary for compliance with a *legal obligation* to which the controller is subject;[21] processing is necessary in order to protect the *vital interests* of the data subject or of another natural person;[22] and in particular processing is necessary for the performance of a task carried out in *the public interest* or in the exercise of official authority vested in the controller.[23]

According to Article 6. 3. the basis for the processing referred for the above-mentioned 'legal obligation' and 'public interest' needs to be laid down in Union law or Member State law to which the controller is subject. This means that consent is not required for data processing activities of public authorities or bodies if the authority or body can demonstrate that the processing is in the 'public interest' and falls within its legal competences.

However, the GDPR restricts the public authorities from using *legitimate interest*[24] as a legal ground for processing personal data. This means that public authorities have to find another legal ground if legitimate interest is currently relied upon.[25] Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. If this is not possible, the personal data may not be processed. Therefore, it is advisable for institutions to assess whether all collected data fall within this scope.

In addition, according to Article 89 of the GDPR processing for "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" is also applicable with appropriate safeguards respecting the principle

[20] GDPR Article 7, 4.

[21] GDPR Article 6, 1 (c).

[22] GDPR Article 6, 1 (d).

[23] GDPR Article 6, 1 (e).

[24] GDPR Article 6, 1 (f).

[25] GDPR Article 6, 1. "Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

of data minimisation and including pseudonymisation provided that those purposes can be fulfilled in that manner.[26]

Rights of the data subject

The intention with creating the GDPR was to establish a strong and more coherent data protection system in the EU based on the responsibilities of the controllers and backed by strong enforcement. However, through the rapid technological development, the data subjects (users) usually cannot understand the functioning of smart devices and applications and cannot see through the route their personal data along the transmission of them. Because of that, natural persons should have control of their own personal data, so it has a high importance of creating the trust of the data subjects with appropriate provisions that will allow the digital economy to develop across the internal market. To achieve this goal the GDPR lays an emphasis on legal and practical certainty for natural persons, economic operators and public authorities.[27]

The GDPR requires the controllers to provide all relevant *information* to data subject in transparent, intelligible and easily accessible form, using clear and plain language when processing personal data.[28] Public authorities might have more freedom than private companies concerning data processing, but they do need to provide also information about the legal basis for processing and with the contact details of the data protection officer and data controller. These contact data need to be communicated to the supervisory authority as well.[29]

The GDPR gives much greater control to data subjects allowing individuals greater visibility of their data with the *right to access* their personal information on request, organizations must be able to meet these requests in a timely manner.[30] Therefore, all data subjects are entitled to make a 'subject access request' (SAR)[31] meaning to obtain confirmation that their data is being processed by the data controller and to have access their personal data on request and organizations are obligated to respond to requests within 30 days under GDPR provisions.

This includes the right for data subjects to have access to data concerning their health, e.g. the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.[32]

[26] GDPR Article 89, 1.

[27] GDPR Recital (7).

[28] GDPR, Article 12, 1.

[29] GDPR, Article 13.

[30] GDPR Recital (63).

[31] IT Governance Privacy Team: EU General Data Protection Regulation (GDPR)–An Implementation and Compliance Guide. IT Governance Publishing, Second edition, Ely, Cambridgeshire, 2017. 222. p.

[32] GDPR Recital (63).

Public bodies will need to ensure that robust data processing systems are in place to cope with the extended rights to the data subject. According to the Recital 63 of the GDPR the controllers shall ensure that data subject in the position "to exercise that right easily and at reasonable intervals."[33] This creates additional administrative work for all organizations within the public sector and upon that public sector organizations should review their procedures and appoint dedicated and qualified staff to deal with SARs.

The right to obtain from the controller without undue delay the *rectification* of inaccurate personal data concerning data subject is under the Article 16 of the GDPR is not a new one, as the right to erasure the so called '*right to be forgotten*'. But latter plays a smaller role in the public sector, compared to other sectors, because it does not applied if it impedes the performance of a task carried out in the public interest[34] (and more specifically in the area of public health)[35] or in the exercise of official authority vested in the controller or the processing is executed for compliance with a Union or Member State legal obligation. These types of processing occur relatively often within the public sector. It also does not apply for data processing for archiving purposes in the public interest, and scientific, statistical or historical research purposes.[36]

In the light of all the above-mentioned situations, it can be stated that for public institutions the legal basis of the processing of personal data is of paramount importance whilst GDPR provides various instruments for public authorities to claim a legal basis or an exception.

As we can observe, while 'consent' and 'the right to be forgotten' are major topics for private sector organizations and entail a complete rethinking of data processing procedures, they generally do not apply to public sector organizations. In this regard, the impact of GDPR is clearly heavier on the private than on the public sector. Therefore, we can conclude that for public authorities working clearly within their legal competence, GDPR does not form an unsurpassable obstacle for the continuation of their normal procedures.

As organizations in the public sector most of the time cannot use freely given consent as a ground for data processing, *data portability* usually only plays a role in contractual relations. Since different grounds are often used for personal data processing within the public sector, than in the private sector, such as processing for performing a task of public interest, data portability has not a major importance in the public sector.[37]

---

[33] GDPR Recital (63).
[34] GDPR Article 17, 3. (b).
[35] GDPR 17, 3. (c).
[36] GDPR 17, 3. (d).
[37] GDPR Article 20, 3.

Data controller's responsibility

The responsibility of the controllers (and processors) processing personal data is emphasised very strongly and covered in detail in the GDPR, therefore this paper concentrates only on the relevant provisions regarding public sector.

Public authorities and bodies as data controllers shall carry out appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR and those measures shall be reviewed and updated where necessary.[38]

These measures shall include the two very important principles*: the data protection by design and by default.*[39] Applying these principles it could be guaranteed that the law builds in the technology. Privacy by design intends to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice or procedures. With privacy by design no action is required on the part of the individual to protect their privacy, because it is built into the system, by default. The result of using this principle is that privacy becomes an essential component of the core functionality being delivered, so privacy is integral to the system, without diminishing functionality.[40] Data protection by default means incorporating these considerations into an existing procedure or system, not just at the beginning. This also can assist to avoid data protection incidents.[41]

It is also an obligation for public authorities to comply with the provisions of GDPR using such systems and technologies while processing personal data, which are created, developed and updated according to the data protection by design and by default principles.

Public authorities or bodies as data controllers are obligated to maintain a special *record of processing activities* under their responsibility, which is a completely new provision under the GDPR.[42] The record shall be in writing, including in electronic form. The special record of processing activities must not be made publicly available, it shall be released to the competent supervisory authority on their request.[43] This record should contain the following information:

– the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

[38] GDPR Article 24.

[39] GDRP Article 25.

[40] Ann Cavoukian: Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices. 2-3. pp. https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf (accessed: 07.03.2019)

[41] Paul B. Lambert: Understanding the New European Data Protection Rules. Taylor&Francis, Auerbach Publications, New York, 2017. 339. p.

[42] GDPR Article 30.

[43] GDPR Article 30, 4.

– the categories of processing carried out on behalf of each controller;

–where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers, the documentation of suitable safeguards;

– where possible, a general description of the technical and organizational security measures.[44]

It is very important to emphasise the obligation regarding the specification the categories of processing operations which are carried out on behalf of the controllers including a description about the services provided by processors. It is also crucial that the information enables an assessment of the degree of risk entered into upon taking the task, so the categories of data recorded by the processing operations should be specified as well as which operations may be concerned.[45]

Upon this information the competent data protection authority will be able to analyse the lawfulness of processing personal data and deliver a decision in case of an incident. The obligation upon request to cooperate with the supervisory authority in the performance of its tasks is enhanced in Article 31 of the GDPR. This cooperation could be an investigation of a personal data breach, which shall be *notified* to the competent supervisory authority by the controller without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[46]

We highlight the obligation of the controller to *document any personal data breaches*, too, comprising the facts relating to the personal data breach, its effects and the remedial action taken,[47] and this documentation shall be provided to the supervisory authority on request.

The GDPR contains another new provision in frame of the controller's responsibility namely the *data protection impact assessment* (DPIA). This means an analysis of the risk of non-compliance to GDPR and is to become standard procedure during the implementation of all processes "likely to result in a high risk to the rights and freedoms of natural person", in particular using new technologies. A Data Protection Assessment contains a "systematic description of the processing and its purposes", an "assessment of the necessity and proportionality of the processing", an "assessment of the risks to the rights and freedoms of data

[44] GDPR Article 30, 2. (a)–(d).

[45] Robert Kazemi: General Data Protection Regulation (GDPR). Tredition GmbH., Hamburg. 2018. 78. p.

[46] GDPR Article 33.

[47] GDPR Article 33, 5.

subjects" and a risk mitigation plan.[48] For public authorities, excluding courts, which process lots of personal data, this entails a new way of preparing to implement almost any significant new technology. These general obligations translate to a whole series of practical measures that need to be taken by public authorities, e.g. need to plan and schedule regular risk assessments to identify any weaknesses in data processing systems to ensure the ongoing security of the data. It is also crucial to take the opportunity to identify all people within organizations who access to personal data and ensure they are thoroughly trained and knowledgeable of the changes and of individuals increased rights to access.

The GDPR provides an assistance for the controller, when the supervisory authority is of the opinion that the intended processing of personal data would infringe the GDPR, where the controller has insufficiently identified or mitigated the risk. In that situation the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller how to handle this situation with appropriate measures.[49]

It should be emphasised that another crucial requirement which is applicable to public authorities and bodies is to appoint a *data protection officer (*DPO), except for courts acting in their judicial capacity.[50] Under the GDPR the DPO is required to monitor processing operations of data subjects or special categories of data on a large scale regularly and systematically.[51]

It is possible for several public authorities or bodies as controllers to designate a single (common) DPO taking account of their organizational structure and size.[52] The DPO shall be well qualified to this position and expert knowledge of data protection law and practices and be able to fulfil the tasks under GDPR,[53] and could be chosen from the staff members of the controller or processor or could be designated on the basis of a service contract.[54] According to the GDPR provisions the DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.[55]

The tasks of the DPO are to cooperate with controller or processor, to advise the organization and employees in relation their data protection obligations under national law and GDPR and to monitor their compliance with the data protection legal regime. The DPO should recommend changes and the various information technologies (IT) (hardware, software, systems, cloud, etc.) used by the organi-

[48] GDPR Article 35, 3.
[49] GDPR Article 36.
[50] GDPR Article 37, 1 (a).
[51] GDPR Article 37, 1 (b), (c).
[52] GDPR Article 37, 3.
[53] GDPR Article 37, 5.
[54] GDPR Article 37, 6.
[55] GDPR Article 38, 5.

zation need to be considered by the DPO as life cycles, storage, disposal and documentation of the personal data.[56] It is possible for each Member State to require additional provisions in their national legislation such as registration of the DPO in a government register. The DPO is also responsible for the communication between the organization and the supervisory authority; and for enforcing the mandatory processes mentioned above.[57] This is different in the private sector, where a DPO is only required when certain criteria are met.

There are some special provisions regarding transfers of personal data to third countries or international organisations from the aspect of public authorities or bodies. This may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.[58]

In the absence of an adequacy decision or of appropriate safeguards pursuant a transfer or a set of transfers of personal data to a third country or an international organisation shall take place when the transfer is necessary for important reasons of public interest.[59]

Conclusion

The GDPR draws special attention to the protection of personal data in the public sector. It introduces a number of significant changes and restrictions. A careful assessment must be done as not all provisions are applicable. Especially the exceptions should be carefully considered before the general rule is applied.

The new regulation empowers the data subject allowing individuals to control their own personal data. Public sector organizations must place their focus on the most important factor, the data subject, whilst also using the opportunity to clear their databases of unnecessary information and provide a better, trustful and more secure service to the public. There is no doubt this is a challenge, and organizations need to consider resourcing levels, technology, training and overall procedures as part of the process.

---

[56] Paul Lambert: The Data Protection Officer: Profession, Rules, and Role. CRC Press, Taylor&Francis Group, New York, 2017. 46. p.

[57] GDPR Article 39, 1 (d).

[58] GDPR Article 45-

[59] GDPR Article 49.

Dr. Szilvia Váradi, egyetemi adjunktus
Szegedi Tudományegyetem
Állam-és Jogtudományi Kar
varadiszilvia@juris.u-szeged.hu

A GDPR hatása a közigazgatásra

Absztrakt: *Az Európai Unió általános adatvédelmi rendelete (GDPR) a kétéves felkészülési időt követően 2018. május 25-én lépett hatályba, és nemcsak a magánszektorra, de a közszférára is jelentős hatást gyakorol ezen idő óta. A GDPR több jelentős változást és szigorítást hozott kifejezetten a közhatalmi szervek és testületek személyes adatkezelési tevékenységére nézve. Az új rendelet fő célja az adatalany személyes adatai feletti ellenőrzési jogának megerősítése, és míg az adatalany hozzájárulása az adatkezeléshez a magánszektorban kiemelkedő jelentőséggel bír, és az adatkezelés egyik jogalapja, addig a közszféra tekintetében több kivételt is találhatunk a magánszektorhoz képest, mint a felejtés joga, az adathordozhatóság, az adatvédelmi hatásvizsgálat, stb. Jelen tanulmány célja a GDPR ezen speciális szabályainak feltárása és elemzése, annak érdekében, hogy a napjainkban is tapasztalható bizonytalanságok feloldhatókká váljanak.*

Kulcsszavak: *GDPR, Európai Unió, személyes adatok védelme, közhatalmi szervek és testületek, közszféra.*

др Силвија Варади, адјункт
Универзитет у Сегедину
Правни факултет
varadiszilvia@juris.u-szeged.hu

Утицај Опште уредбе о заштити података на јавну управу

Сажетак: *Општа уредба о заштити података Европске уније ступила је на снагу након двогодишњег периода, 25. маја 2018. године и од тада има снажан утицај не само на приватне него и на организације јавног сектора. Општа уредба о заштити података уводи много значајних промена и ограничења која се односе на поступање јавних власти и тела. Ова нова уредба оснажује субјекте података да контролишу употребу сопствених личних података, и док пристанак субјекта података (корисника услуге) представља један од основних правних основа за обраду личних података, постоји много изузетака за јавни сектор, као што је такозвано право да се буде заборављен, преносивост података, процена утицаја на заштиту података и тако даље. Циљ овог рада је да истражи ове посебне одредбе и анализира их да би разјаснио неизвесност која још увек постоји у овој области.*

Кључне речи: *Општа уредба о заштити података, Евроска унија, заштита личних података, јавне власти и тела, јавни сектор.*