SCIENTIFIC REVIEW PAPER

UDK: 340
Primljeno: srpanj 2020.

NIKOLA PROTRKA*, KRISTINA GODANJ**

Relationship between the interests of the individuals and the right of erasure of personal data

Abstract

The subject of this article is an aspect of personal data protection, the data subject's right of erasure, or respectively the „right to be forgotten". The rights of the data subjects concerning the protection of personal data have been more clearly defined. One of the most important of those rights is the right of erasure, resulting in reaffirmation and strengthening of the active role of the subject in all phases of personal data processing. Besides outlining and commenting on the conditions required in order to consume this right, the article explains the delicate relationship between the interests of the individuals and the right of erasure of personal data of the subject with the public or individuals' right of access to information together with possible conflicts as a result. There is also a comparison between the right to erasure and the right to rehabilitation from the perspective of penology.

Keywords: *General data protection regulation; GDPR; personal data; the right to erasure; the right to rehabilitation.*

INTRODUCTION

The reason behind the implementation of the General Regulation on Data Protection (GDPR) - Regulation (EU) 2016/679 (hereinafter: the Regulation) was around privacy issues after the adoption the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 27, 2016 on the protection of 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) GDPR. This article sets out to show how the subject (a member of the public or of an organisation) is protected and explains the stringent rules in place. This

* dr. sc. Nikola Protrka, Ministry of the Interior, Police College, Zagreb, Croatia.

** Kristina Godanj, Ministry of the Interior, Police station Jastrebarsko, Zagreb, Croatia.

legislation gives the subject more control over their own information. The GDPR generally sets out seven principles around collection, organisation, structuring, storage, alteration, consultation, communication, combination, restriction and the subject of this article the right to erasure or destruction of data. The Regulation started by the end of May 2018, after a two-year delay period in order to regulate the use of the personal data and the right to privacy within the framework of the contemporary society. It affects the digitalization in all spheres of life and thus threatening the individual's freedom and rights. The enactment of the Regulation strengthens the rights of the data subject, respectively the individual to whom the data are related, by prescribing the conditions of the collection of the personal data of an individual and by protecting the interests of the data subject.

THE EMERGENCE OF THE RIGHT TO ERASURE AND ITS LEGAL FRAMEWORK WITHIN THE REGULATION (EU) 2016/679

According to the Regulation, the definition of the personal data says that *"...personal data means any information relating to an identified or identifiable natural person ('data subject'), an identifiable natural person is one who can be identified, directly or indirectly, 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, psychological, genetic, mental, economic, cultural or social identity of that natural person."*. Thus, the range of the data which are considered as the personal data increased comparing to the previous period and all that in order to achieve the higher level of their protection. Directive 95/46/EU of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data in the Article 2 says that *"...'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."* Regardless to the reaction of the public after the enactment of the Regulation and the impression that the Regulation imposes some new rules and obligations, the question of the data protection is not new. At the time of foundation of the European Community for Coal and Steel in 1951 in order to meet the common economic interests, one of the key issues that required the regulation was the matter of the protection of personal data in the process of the exchange between the member states in their cooperation.

Therefore, in 1953 the European Convention on Human Rights and Fundamental Freedoms (hereinafter: ECHR) was dealing with privacy. The Article 8 of the ECHR says that *"Everyone has the right to respect for his private and family life, his home and his correspondence."* and that *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."* Besides the personal data protection, respectively the protection of *the privacy*, ECHR relates to the other fundamental human rights and the supervision of their respect is in charge of European Court of Human Rights in Strasbourg, which was established in 1959. After that, in 1981, The Convention

for the Protection of Individuals with Regard to the Processing of Personal Data of the Council of Europe (hereinafter: Convention 108), which relates to the protection of the personal data exclusively in order to achieve uniformity of processing in all member states. Subsequently in 1995 the Directive 95/46/EC was enacted with the purpose of providing both the protection and the free flow of personal data exchange at the same time what is described in the Article 1 of the Directive 95/46/EC. The next step in the development of the data protection within the European Union (hereinafter: EU) represents the Charter on Fundamental Rights of the European Union (hereinafter: the Charter) in 2000 which, apart from the protection of personal data, deals with other fundamental human rights as well. Unlike the Convention 108, the Charter fails to mention about the achievement of higher unity between the member states; instead, it speaks about the common values that arise from the national legislation and practice of the European Union and its member states. In the preamble of the Charter it says that *"This Charter reaffirms, with due regard for the powers and tasks of the Union and for the principle of subsidiarity, the rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Social Charters adopted by the Union and by the Council of Europe and the case-law of the Court of Justice of the European Union and of the European Court of Human Rights. In this context the Charter will be interpreted by the courts of the Union and the Member States with due regard to the explanations prepared under the authority of the Praesidium of the Convention which drafted the Charter and updated under the responsibility of the Praesidium of the European Convention."* The fields which are covered by the Charter are divided into the freedom, equality, solidarity, citizens' rights and justice. Article 8 of the Charter defines the right of data protection as a fundamental human right, respectively as *the right of each individual.* The same article regulates that the data must be processed *fairly*, for *specified purposes* exclusively and *on the basis of the consent* of the person concerned or on another *legitimate basis*. Furthermore, each person has the right of *access to data* that is related to that person and the right to have it *rectified*. The control of compliance with these rules is the task of an *independent authority.* EU Charter of fundamental rights says: *"Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority."* Although those explanations do not as such have the status of law, they can be a valuable tool of interpretation intended to clarify the provisions of the Charter.

IMAPCT OF A DIGITAL TECHNOLOGY

Digital technology has made a great impact on everyday life and business, while the law has struggled to adjust of the scale of change. The legal framework regarding personal data protection resulted in the enactment of the Regulation. One could ask the question: why does the Regulation replace the Directive? The reason is simple - although both legal instruments are binding, there is a huge difference between them: a directive defines the goal to be achieved by the member states without defining the manner of achieving the goal unlike the Regulation

which must be applied directly. Thus the European Union raised the issue of personal data protection on the highest possible level, since the enactment of the Regulation it compelled all member states to the consistent implementation of the unique legal instrument. Furthermore, it resolved the disparity of legal provision and the problem of the legal uncertainty that represented an obstacle to the cooperation of different member states of European Union because certain activities during the processing of personal data were legal in some states and illegal in others (Galea, 2015). Therefore, the main issue in the future will not be the unique legal framework, but the unique implementation of the provisions of the Regulation that should be the assignment of the European Data Protection Board on the EU level and the Agency for Data Protection on the national level in the EU states. European Data Protection Board is described and explained as *"...will be at the centre of the new data protection landscape in the EU. It will help ensure that the data protection law is applied consistently across the EU and work to ensure effective cooperation amongst DPAs (The data processing agreement). The Board will not only issue guidelines on the interpretation of core concepts of the GDPR but also be called to rule by binding decisions on disputes regarding cross-border processing, ensuring therefore a uniform application of EU rules to avoid the same case potentially being dealt with differently across various jurisdictions."*

The right on personal data protection in EU legislation, as previously mentioned, is considered as a fundamental human right. This right is always tightly connected to the right on privacy since it is in fact a derivation, so the laws that imply the personal data protection are often called the laws on privacy protection. In her book *"The Emergence of Personal Data Protection as the Fundamental Right in EU",* Gonzales Fuster says that we should always keep in mind the fact that the provisions on personal data protection in EU legislation primarily serve the right on privacy, which is also the reason why the EU Court often does not differ the personal data protection from the right to the respect of the private life cited *"The EU Court of Justice had indeed ruled that, in order to apply EU personal data protection laws, it must always be remembered that they serve the right to privacy, and, thus, what must be applied is (directly, simply, exclusively) the right to respect for private life of Article 8 of the ECHR. From this perspective, the Luxembourg Court has occasionally not recognised any relevant difference between EU personal data protection and the right to respect for private life — in what can be described as operations of coupling of legal notions, or of legal indistinction."* (Fuster, 2014:59). The Court of Justice of the European Union is an institution which is based in Luxembourg and it has a double role: it must provide the uniformity of the implementation of the EU legislation in all member states on one side and settle the legal disputes among the member states and the EU on the other side. It also handles the lawsuits of the individuals, companies or organisations against the institutions of the EU if they consider that they violated some of their rights.

The right of personal data protection developed in its present shape gradually, due to political, economic, social and technological factors, as well as the legal framework and judicial practice. It is realistic to expect that these changes and the mutual interference will continue in the future, too. The absolute right on the personal data protection of an individual would mean that the individual has no obligation to share his or her personal data with anybody since he or she has the right of complete anonymity. This would lead to a conflict between the interests of the society and the individual, because the interests of the individual would be fully met from one side, and the functionality of the society would potentially be harmed on the other side. Data protection, therefore, does not represent a prohibition of the use of

the personal data, but imposes a limitation on the amount of data collected and imposes the necessity rule for a certain purpose instead. At the same time, it requires a transparently developed system of limitation of the data subject's rights under the clear conditions and control of the inspecting authority and courts. Therefore, the Regulation determines the framework which defines the acting of the controller and the rights of the data subject whose data are being processed, which include now the explicitly regulated rights - the components of the right on the data protection. Those can be, for example, the right to transparency and information on processing, the right of access to the data, the right on rectification and erasure (so called "the right to be forgotten"), the right to data portability, the right to object and the right to oppose the automated individual making of decisions which influence the subject data (so called profiling) (Garcia, M.A.F. 2020).

The right to rectification and erasure can freely be considered as a kind of corrective right, since its purpose is the repair of the unfavourable processing situation that occurred because of certain mistakes during the data processing. It represents a protective mechanism that can be used by the data subject in order to influence the processing of his or her personal data after the beginning of the process. This right is necessary because the data processing has a negative impact on the rights and freedoms of the data subject, especially in case of inaccurate or incomplete data. Since the right to rectification and erasure of personal data covers the scope that is tightly linked, this area is commonly covered by the text of the Regulation in Section 3. Besides, the same Section sets the provisions on the *right to restriction of the amount of the data* that can be used as a kind of compromise between the interests of the data subject and the controller and the *right to portability of the data.* One of the most important principles in the implementation of the Directive is the principle of the *correctness and accuracy.* Incorrect data are the data that do not reflect the reality. Although the incomplete data are correct, they are not sufficient to make the right and unambiguous conclusion. The selection of the right to which the data subject would appeal depends on the will of the data subject and the circumstances of the certain case keeping in mind the fact that the primary goal of the right to the rectification and erasure of the personal data is the correction of the cases where the law was broken. The data subject is not obliged to give specific reasons for the demand of its application, instead he or she must only submit the *evidence* which prove the incompleteness or incorrectness of the data. The data that does not reflect the reality must be rectified by the controller without delay. The cases where the data is being processed on the basis of the controller's assessment remain disputable, because their inaccuracy should be proven in order to enable the data subject to consume his right to the rectification of such data. The data subject has the right to the rectification or erasure of the data that refer to himself of herself. (Gutwirth et al. 2015).

At first, the act of completing the data may seem to be less invasive and problematic comparing to the deletion of the data. However, there are also certain rules that must be obeyed. One of the basic problems is the danger of the storage of the redundant oversized data that is contrary to the principle of the data minimisation. Additionally, the rationality of the data completion can be disputable if it results in the disproportional expenses and difficulties compared to the benefits. Finally, it is also important to take into account the possible damage for the data subject. Therefore, the criteria for the data completion can be summed up by the following conditions: the completion is necessary in order to achieve *the purpose of the data processing*, the completion justifies the need for the investment of the *additional effort* and the degree of the possible *damage* for the data subject in case if the completion does

not take place. The data subject can carry out the completion of his or her personal data by submitting the additional statement and the time limit for the controller to execute it has not been defined, instead the term "without the unnecessary delay" is used. This means that the controller must execute the completion immediately after the expression of the will of the data subject or allow the data subject to execute the completion or rectification of the data by the registration and accession to the data within the system of the data controller.

ADMINISTRATIVE PRACTICE

As the Regulation came into force, the *right to erasure (i.e. "the right to be forgotten")* drew the interest of the public. The right to erasure became an important issue in 2014 as the Court of Justice of the European Union pronounced a judgement in case of the Spanish citizen Mario Costeja Gonzalez. Namely, it concerns the case in which the Spanish lawyer Costeja Gonzalez on March 5, 2010 demanded the popular Spanish newspaper "La Vanguardia" and companies Google Spain and Google Inc. to erase his personal data relating to the auction of the real estate, due to negative publicity and reputational damage caused by social insurance debts which showed up on the websites in search engines with his name. The article had taken place in 1998, so the data about it was neither relevant nor in the interest of the public. The data subject was distressed and that is why he requested the erasure or concealment of his personal data regarding the case that was approved later by the Court of Justice of the European Union (EUR-Lex. Right to be forgotten on the Internet, 2014). This judgement also played a very important role in the process of enacting the Regulation and became incorporated and additionally widened as the controller was compelled to take all the reasonable measures in order to make the third parties who received the personal data of the subject to act in accordance with the will of the data subject. The judgement says that the provider of the service of the search engine can be compelled to *remove all the links* to certain websites from the list of results that show up during the search of the certain name, which means that the disputable data are not in fact erased, but they are less accessible in order to protect the interests of the data subject. As follows, it is obvious that it is very hard to accomplish the complete erasure of the data once they have been used. The Court of Justice of the European Union stated in the same judgement that the data subject's right to be excluded from the results of the search on the basis of his or her name must be applied in case of the *inaccurate, inappropriate, insignificant or the data which became irrelevant,* as well as in cases of *redundant* data, in other words, in cases of violating the principle of the data minimisation.

Despite that, it is obvious that the consumption of the right to erasure of the personal data is not the matter of automatism. As illustration, we can take into consideration the case of Chamber of Commerce v Salvatore Manni where the Italian High Court of Cassation requested a preliminary ruling from the European Court of Human Rights regarding Salvatore Manni's request to erasure, anonymisation or restriction of his personal data in the public register of the Chamber (EUR-Lex, Judgement of the Court (Second Chamber), 2017). Namely, Salvatore Manni was the sole director of "Italiana Construzioni Srl", the company that constructed a tourist complex, but he had difficulties with the selling of the complex. In his opinion, his business problems originated from the fact that his personal data were stored and accessible to the third parties from the public register of the Chamber of Commerce in Lecce. These data implied that he had been the sole director and liquidator of "Imobiliare e

Finanziaria Salentina Srl", the company which had become insolvent in 1992 and struck off the companies register, finishing up with the liquidation proceedings in 2005.

However, his request was not adopted due to several reasons. Despite the fact that his former company did not exist anymore, "…*the rights and legal relations relating to it continued to exist,*" so the contentious data was still relevant (Information Note 205. Case-Law of the European Court of Human Rights, 2017). Regarding the limitation of the period of the data processing, it was regulated differently in each Member state of the EU and it could not be precisely determined. Considering the amount restriction of the personal data, the register contained only the necessary data (identity and respective functions of the persons involved) and thus the amount restriction had been fully respected. The register was the irreplaceable tool that helped natural persons to make decisions about their possible business engagement with different companies and thus it justified its existence. Therefore, we can say that in this case the public interest to access the information prevailed over the individual's interest to the protection of his personal data, which is additionally explained in the Conclusion.

RELATIONSHIP BETWEEN RIGHT OF ERASURE AND THE RIGHT TO REHABILITATION FROM THE PERSPECTIVE OF PENOLOGY IN THE REPUBLIC OF CROATIA

From the superficial point of view, the right to erasure has a lot in common with the right to rehabilitation. The right to rehabilitation belongs to the sphere of penology. Unlike the right to erasure, it does not refer to the entire population, but to the offenders only. The penology must meet two basic demands: the retribution on one side and the reintegration of the offenders afterwards on the other side. Here we will explain situation in The Republic of Croatia. According to the Article 18 of the Law on Legal Consequences of the Sentence, Criminal Records and Rehabilitation (hereinafter: LLCSRR): *"The offender of the crime who is finally convicted or released from the punishment has the right, after passing of time in accordance with the law and under the conditions which are regulated by this Law to be considered as person who did not commit a crime, and his/her rights and freedoms cannot differ from the rights and freedoms of persons who did not commit a crime."* Thereafter, the provisions of the LLCSCRR precise in which periods the right to rehabilitation comes into force under the condition that the offender of the crime is not convicted again for another crime in the meantime. *"After the expiration of the periods which are determined in the paragraph 4 of this article the offender of the crime is being considered as a non-convicted person and each use of his/her data as an offender of the crime is forbidden, and the use of those data has no legal effect. The rehabilitated person has the right to deny his/her former convictions and must neither be called to responsibility for that, nor suffer any other legal effects."*

The Ministry of Justice of the Republic of Croatia issues the decision on rehabilitation *by the official duty* when the rehabilitation comes into force after the time which is fixed by the law has passed and in case if the convicted person has not committed another crime. All this implies that the right to rehabilitation is in fact a kind of the right to the erasure of the data. After the erasure of his/her personal data from the criminal records, the person who obtained the decision on rehabilitation can completely justifiably demand the removal of his/her personal data from all data basis considering his/her criminal past.

CONCLUSION

Unlike the right to rehabilitation, the consumption of the right to the data erasure is not conditioned by the time limitations and is cannot be applied by the official duty, but on the initiative of the data subject. Despite that, both consumption of the right to rehabilitation and the right to erasure enable the individuals to carry on with their lives without the burdens from the past.

The scope of information that can be found about some individual from so many sources by analytics companies is mind-boggling. Everything from what your buying patterns are, what webpages you've visited, what events you've attended, where you live, what your income is, who you connect with on social media, where you live, which people you had relationships with, and much more is available across cyberspace. After submitting the request for erasure of the personal data, the controller ought to make the assessment of the relation between the interests of the data subject and the public interest for the access to the information. One of the basic criteria the controller must keep in mind in that case is the role of the individual in the public life. This is the way of preventing the removal of the information about the public persons or organisations simply because they do not suit them. The complexity of the relationship between the right of the individual to request erasure of his/her data and the right of access to information requires further development of practice, both on the national and European Union level. In order to avoid the situation in which the controller makes the assessment of the request for erasure alone, because of possible subjectivity and partiality, the process must be supervised by the independent national inspecting authority for the data protection. This judgement had the key role in the process of forming the standards of the Regulation regarding the right to the erasure of the data.

REFERENCES

1. Biloš, A., Turkalj, D. i Kelić, I. (2019). Implementacija Opće uredbe o zaštiti podataka pri EU: Preliminarna analiza aktualnih istraživačkih napora i izazova. CroDiM, 2 (1), 1-15. Preuzeto s https://hrcak.srce.hr/234528
2. Charter on Fundamental Rights of the European Union. 2007/C.303/01. URL: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:12007P (29.10.2018.)
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. URL: https://rm.coe.int/1680078b37 (29.10.18.)
4. EUR-Lex, Judgement of the Court (Second Chamber), 9 March 2017, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni. URL: https://eur-lex.europa.eu/legal-content/GA/SUM/?uri=CELEX:62015CJ0398 (20.06.2020)
5. EUR-Lex. (2014) Right to be forgotten on the Internet. URL: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=LEGISSUM%3A310401_1 (20.06.2020.)
6. EUR-Lex. Judgement of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. URL: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A62012CJ0131 (20.06.2020.)

7. European Commission. What is the European Data Protection Board (EDPB)? URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_hr. (20.06.2020.)
8. European Convention on Human Rights and Fundamental Freedoms Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. URL: https://rm.coe.int/1680078b37 (20.06.2020.)
9. European Parliament (2016). 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). URL: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 (20.06.2020.)
10. Galea, M. (2015). The Right to be Forgotten; a balance between privacy and public rights? University of Malta.
11. Garcia, M.A.F. (2020). The comparison of corrective powers of the supervisory authorities in the Modernized Convention 108 and the GDPR – a new minimalist approach? University of Luxembourg.
12. Gonzalez Fuster, G. (2014). The Emergence of Personal Data Protection as a Fundamental Right in the EU". Page 259. Springer. Cham. Switzerland.
13. Gutwirth, Serge, Leenes, Ronald, de Hert, Paul. (2015) Reforming European Data Protection Law Volume 20. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. Springer Science. URL: https://art1lib.org/ireader/41086148 pp. 171-180 (20.06.2020.)
14. Information Commisioner's Office. Right to object. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/ (20.06.2020.)
15. Information Note 205. Case-Law of the European Court of Human Rights. March 2017. Other Jurisdictions. Page 33. URL: https://www.echr.coe.int/Documents/CLIN_2017_03_205_ENG.pdf (20.06.2020)
16. Mladinić, A., Puljak, L. i Koporc, Z. (2021). Post-GDPR survey of data protection officers in research and non-research institutions in Croatia: a cross-sectional study. Biochemia Medica, 31 (3), 0-0. https://doi.org/10.11613/BM.2021.030703
17. Ochodek, T. (2019). The right to erasure: what is the framework given to eu member states? The Lawyer Quarterly, Vol 9, No 1. 2019. https://tlq.ilaw.cas.cz/index.php/tlq/article/view/316 (20.06.2020)
18. Official Gazette of the Republic of Croatia. (2017) Law on Legal Consequences of the Sentence, Criminal Records and Rehabilitation. Narodne novine 143/12., 105/15., 32/17.
19. Puljak, L., Mladinić, A., Iphofen, R. i Koporc, Z. (2020). Before and after enforcement of GDPR: Personal data protection requests received by Croatian Personal Data Protection Agency from academic and research institutions. Biochemia Medica, 30 (3), 363-370. https://doi.org/10.11613/BM.2020.030201
20. Pelekanos, A. (2015). The Latest Developments Regarding the "Right to be forgotten". University of Sussex.
21. Škrinjarić, B., Budak, J. i Rajh, E. (2019). Perceived quality of privacy protection regulations and online privacy concern. Economic research - Ekonomska istraživanja, 32 (1), 982-1000. https://doi.org/10.1080/1331677X.2019.1585272

22. Tsesis, Alexander (2019). Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure. Loyola University Chicago School of Law. URL: https://art1lib.org/ireader/75766141 pp. 593-602 (20.06.2020.)
23. T.F.E. Tjong Tjin Tai. The Right to be forgotten. (2016). International Review of Law, Computers & Technology .Volume 30, 2016 - Issue 1-2.
24. Thomson Reuters (2021). Right to be forgotten - erasing your private information from cyberspace. https://legal.thomsonreuters.com/en/insights/articles/erasing-your-private-information-from-cyberspace (20.06.2021.)
25. Voigt, P., Von dem Busche, A. (2017). The EU General Data Protection Regulation, A Practical Guide, page 158. Springer, Cham, Switzerland, 2017.

Sažetak

Nikola Protrka, Kristina Godanj

Povezanost interesa pojedinaca i pravo na brisanje osobnih podataka

Tema je ovoga članka pogled na zaštitu osobnih podataka, pravo na brisanje osobnih podataka pojedinca, to jest ,,pravo na zaborav''. Jasnije su određena prava pojedinaca na zaštitu osobnih podataka. Pravo na brisanje jedno je od najvažnijih prava vezanih uz zaštitu podataka. To pravo dovodi do ponovnog potvrđivanja i jačanja aktivne uloge pojedinca u svim fazama obrade osobnih podataka. Osim pregleda i tumačenja uvjeta koji su potrebni kako bi se koristilo to pravo - ovaj članak govori i o osjetljivoj povezanosti interesa pojedinaca i prava na brisanje osobnih podataka pojedinca u javnosti; kao i o pravima pojedinaca na pristup informacijama iz kojeg može doći do mogućih sukoba. Članak sadrži i usporedbu prava na brisanje i prava na obnovu podataka iz perspektive penologije.

Ključne riječi: Opća uredba o zaštiti podataka, GDPR, osobni podaci, pravo na brisanje, pravo na obnovu podataka.