ŠTO? QUIS? ГДЕ? QUAND? COME? WITH WHAT? WARUM

MEĐUNARODNO KRIMINALISTIČKO • UDRUŽENJE INTERNATIONAL CRIMINALISTIC • ASSOCIATION

KRIMINALISTIČKA TEORIJA I PRAKSA

CRIMINALISTIC THEORY AND PRACTICE

ISSN 1849 - 6164
god. 8., br. 15., str. 1 – 97., Zagreb, 2021.

KRIMINALISTIČKA TEORIJA I PRAKSA
CRIMINALISTIC THEORY AND PRACTICE
god. 8., br. 15., str. 1 - 97.,
Zagreb, 2021
polugodišnjak / semiannually

Nakladnik / Publisher
Međunarodno kriminalističko udruženje /
International Criminalistic Association

Uredništvo / Editorial board
prof. dr. sc. Marija Lučić Ćatić, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Univerzitet u Sarajevu
prof. dr. Oliver Lajić, Kriminalističko-policijski univerzitet, Beograd
prof. dr. Ivana Bjelovuk, Kriminalističko-policijski univerzitet, Beograd
doc. dr. sc. Josip Pavliček, Visoka policijska škola, Zagreb
dr. Slobodan Oklevski, Ministarstvo unutarnjih poslova Republike Sjeverne Makedonije

Glavni urednik / Editor-in-chief
dr. sc. Lana Milivojević, Visoka policijska škola, Zagreb,

Tehnički urednici / Technical editors
Matej Podboj
Andra Žic

Dizajn / Design
Matej Podboj

Naslovnica / Cover
Međunarodno kriminalističko udruženje

Indeksiranje / Indexing
Central & Eastern European Academic Source (CEEAS)
EBSCO Discovery Service (EDS)

WEB ADRESA ONLINE IZDANJA
http://criminalisticassociation.org/projekti/casopis-kriminalisticka-teorijai-praksa
Adresa uredništva / Address of editorial board
Međunarodno kriminalističko udruženje,
Vlaška 72a, 10 000 Zagreb, Republika Hrvatska
e-mail: info@criminalisticassociation.org
web: www.criminalisticassociation.org
Članci nisu lektorirani / Articles are not proofread

SADRŽAJ:

CONTENTS:

UDK:24-266:005.922.1:001.103

Nikola Protrka
Ministry of the Interior, Police College, Zagreb, Croatia
nprotrka@mup.hr

Kristina Godanj
Ministry of the Interior, Zagreb, Croatia
kgodanj@mup.hr

Exploring the right to be forgotten in a digital world

The General Data Protection Regulation (GDPR) in Europe regulates erasure obligations. This grew out of the test case that derives from the case Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González (2014). This codified the right to erasure obligations. Personal data must be erased immediately where the data is no longer required for their original purpose, or where consent has been withdrawn. This includes where the data subject has objected and there are no legitimate grounds for the processing. The data subject moves from a passive role in the past to now being an active subject. Their will has a strong impact on the processing of his/her data. It is especially important, when it comes to the fundamental rights of data subjects that rights are clearly defined by the Regulations. The main reason for pursuing these provisions is to protect data subjects in a society where information technology has become a huge part of everyday life. This article seeks to explain the rights of the individual citizen and the responsibilities of organisations. The article also explains the difficulties in applying these principles.

***Keywords**: The right to be forgotten, GDPR, personal data, Google*

1. INTRODUCTION

The right to erasure of the data or so called "the right to be forgotten" can be defined as the right which enables the data subject to have his or her personal data erased if they do not want further processing of his/her personal data. If the controller of the data within a company or organisation no longer has legitimate reasons for further processing that data.[1] The right under the General Regulation on Data Protection (GDPR) - Regulation (EU) 2016/679 (hereinafter: The Regulation) issued in 2018 meant that members of the public can make a request verbally or in writing. The regulation also sets out erasure statutory obligations under the EU law. Data must be erased if the processing itself was against the law in the first place. In addition, the right to be forgotten is found in Article 17(2) of the GDPR. This right to erasure does not refer to the erasure of the incorrect data, because the controller's official duty is to pay attention to the correctness of the data, otherwise it is his duty to erase them without delay.[2] The right to be forgotten has been at the centre of a debate about balancing privacy and free speech in the internet age. In Europe, both principles are written into the European Union Constitution.

Advocates of the new law say the policy is a much-needed legal tool for people to have personal information removed, while critics say different countries are interpreting the law differently. The right to be forgotten has been at the centre of a debate about balancing privacy and free speech in the internet age.

In order to invoke the right to erasure of personal data at least one of the following conditions must be met:

- personal data is no longer necessary to the fulfilment of the purpose of their initial collection

In this case the main assumption is that the data was legally collected and processed in the beginning. However, after a certain time the data is no longer necessary for the purpose of that collection. In this case the purpose of the collection no longer exists, it is therefore necessary to verify if the disputed data is required for the original purpose for which it was collected. If it partially covers or has been adjusted from that original purpose of the data collection and processing, then erasure of the data will not take place.

- withdrawal of the consent which the data subject submitted previously to the controller regarding the processing of his data

[1] In order to avoid the ambiguity and inequality in the implementation of the provisions of the Regulation regarding the consent, the European Commission had founded a working party which created the Guidelines on Consent under Regulation 2016/679. In the meantime the mentioned working party was dismissed and the European Data Protection Board (EDPD) carries out the control and the harmonization of the implementation of the Regulation. (European Commission. *Guidelines on consent under Regulation 2016/679 (wp259rev.01)*. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (10.08.2019.))

[2] The Regulation, Art. 5 (1c)

2. THE RIGHT TO BE FORGOTTEN AND ITS LEGAL FRAMEWORK WITHIN THE REGULATION (EU) 2016/679

Processing of the personal data can be based on the consent or any other legal ground.[3] When the processing is based on consent, the data processing controller must prove the existence of the data subject's consent. The text of the consent must be written in a simple and clear language so that the data subject, even if he or she is a child, can fully understand what personal data is being collected, as well as the purpose and the consequences of the collection. The burden of proof therefore that the personal data of the subject has been collected legally is challenging in the scope of the Internet, because the Regulation does not set out precisely the provisions of the formal requests for its' collection. The data subject can withdraw his/her consent at any moment, which then dictates the reason to cease the data processing. The data subject can also demand the erasure of his/her data on the basis of the withdrawal of the consent. The data subject must be informed about the right to withdraw his/her consent any time before issuing their consent, the withdrawal procedure should be as simple as giving consent.[4] Besides that, the data subject can appeal to the non-existence or invalidity of the consent. For example, the consent which was not signed willingly by the data subject and under the threat of repercussions is invalid. Such a situation is obvious when there is a huge disparity of power between the data subject and the controller (for instance, a citizen in relation to the governmental authorities). Also, each data processing procedure demands a separate consent.[5] The withdrawal of the data subject's consent does not mean that the previous data processing was illegal, but in case the consent was the only legal ground for its processing, the continuance of the processing would definitely be illegal.[6]

The right implementation of the Regulation provisions regarding the obtaining of the consent in a simple and clear way is explained on the website of office of the Information Commissioner's Office (hereinafter: ICO).[7] ICO is the UK independent body whose domain is the protection the right of information in the public interest and transparency of the public administration bodies and protection. The ICO is further concerned about the privacy of individuals in the United Kingdom.

[3] Ibid., Art. 7 and 8

[4] Ibid., Art. 13 (2 c)

[5] In the preamble statement, line 43 of the Regulation, it is stated that *„In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case* ***where there is a clear imbalance*** *between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow* ***separate consent*** *to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."*

[6] The Regulation, Art. 7 (3) – *"The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."*

[7] Information Commissioner's Office. *Consent*. URL: .https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (10.08.2019.)

Regarding consent, the ICO emphasizes the high standards for obtaining the consent, which actually means that the consent must be completely unambiguous. The consent must express the clear and affirmative attitude of the data subject and must be separate from other forms: it should not be used as a precondition for the use of a service. Before obtaining consent, it is necessary to inform the data subject about his/her right to withdrawal and the way he/she can exercise this right. The central tenet of the Regulation is the importance of consent. It represents the legal ground of data processing. Valid consent must contain the following elements: voluntariness; the expression of the affirmative action - the will of the data subject; data about the controller; the purpose and types of processing and periodic revisions of the consent's validity.

Children enjoy a special category with a special kind of protection because the provisions of the child's consent are additionally restrictive. The minimum age of a child who can give his/her consent varies from one EU member state to another (from thirteen to sixteen years).[8] If the child is younger, the consent can be given by the holder of the parental responsibility. The controller must take all reasonable measures, which are not actually defined by the Regulation, in order to reveal the real age of the child and the identity of the holder of the parental responsibility. It must be stressed out that these provisions are generally applicable to the contents which are specially designed for children (for instance, the cartoons, children's encyclopaedia, etc.) which can be derived from the formulation that it can be applied in relation to the offer of the information society services directly to a child. Practically, the demands for verification of the age of the data subject and the identity of the holder of parental responsibility represent a huge problem in the area of the Internet services, because generally, the controller and the data subject are not physically at the same place. Because of the fact that the child can be unaware of the consequences of giving consent, the data subject can withdraw consent they gave as children even after the requisite age, and so exercise the right to the data erasure. Although they are not mentioned as a separate vulnerable group for consent purposes they are seen as a vulnerable group along with the elderly and those with mental health issues. Digital technology can expose their weaknesses and society along with the Police must be there to protect them especially if the data subject withdraws their consent and there are no other legal grounds for further data processing. This concerns the cases when the data subject withdraws their consent which is the basis for the data processing and there are no other legal grounds for the further processing apart from the consent itself. The data subject has the right to withdraw his/her consent at any moment, which makes further data processing illegal.[9] Accordingly, the data subject has the right to the erasure of their personal data.

- if the data subject objects relating to his/her personal data processing in accordance with the article 21 paragraph 1 while the stronger legitimate reasons for processing do not exist or if the data subject objects the data processing in accordance with the article 21

[8] The Regulation, Art. 8 (1)
[9] Ibid., Art. 7 (3)

paragraph 2.

The data subject has the right to submit their objection to the controller, that is the request to cease the processing of his/her data.[10] This right can be implemented under certain conditions, especially if conducted in the public interest or if the controller is a public administrative body . They can also object for other legitimate interests Nevertheless, if it concerns the data processing in scientific, historical or statistical purposes the right to object is restricted.

If direct marketing is not concerned, the data subject has the right to request termination of his/her data processing at any moment and his/her request must be respected.[11] Despite that, the immediate erasure of the personal data is not necessary, but it is sufficient to keep those data separately with the remark that the data subject doesn't want his/her personal data to be used for that purpose in the future.

If the data subject objects to the processing of his/her personal data and the processing is performed in the public interest, by a public administrative body because of the legitimate interests of the controller or the third persons, the data subject must point out the concrete reasons for his/her objection in each individual case. The controller must make the assessment whether the reasons which were pointed out by the data subject were justified or not. During the assessment, the controller must keep in mind the reasons for the objection (e.g., if the data subject suffers the material damage) and other details of the case (e.g. if is a child) and try to balance the interests, rights and freedoms of the controller to the interests of the processing. The controller is obliged to inform the data subject about his/her decision regarding the objection and give the reasons for such a decision. The controller must also inform the data subject about his/her right to object to the supervisory authority or to start a court procedure. The controller can carry on with the data processing if he/she is able to prove the existence of the binding legitimate reasons which override the interests of the data subject and if the procedure is necessary for the establishment, exercise or defence of the legal demands.

When it concerns a personal data procedure in scientific, historical or statistical purposes, the right to object is restricted.[12] Instead of ceasing with the data processing, the data subject's demands can be met by the alternative methods of the data protection, such as minimisation or pseudonymisation of the data.[13]

If personal data is being processed in the purpose of the direct market, for the public interests or performed by body of the public authority, during his/her first contact with the data subject the

[10] The Regulation, Art. 21 (1): *"The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."*

[11] The Regulation, Art. 21 (2)

[12] The Regulation, Art. 21 (6)

[13] Ibid., Art. 25

controller is obliged to specifically inform him/her on the right to object. In cases when data are being processed for the scientific research or statistical purposes, the controller must state the right to objection among other information relating to the rights of the data subject.[14]

Illegal data processing is the raison d'être for erasing the data and it means that any violation of the law is inadmissible. To define Lawful data processing, the Regulation determines that the processing is lawful only when at least one of the following conditions is fulfilled:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 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;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[15]

The provision corresponding to the erasure of the personal data in case of unlawful data processing enables the data subject to use the right to the erasure both in case if it concerns the lack of the lawful foundation or the non-compliance to the provisions of the Regulation. For example, the data procedure can be unlawful if the controller does not fulfil the standards of the data protection, if there are some organizational disadvantages and so on.[16]

- the erasure of the personal data because of the the legal bindings of the European Union or its' member state

The existence of the legal provisions, i.e. the legislation of the European Union and its' member state to erase personal data in certain cases represent the lawful grounds to implement the "right to be forgotten." So, in cases when the national legislative of a certain EU member state requires the obligation to erase the personal data, the controller must carry it out.

---

[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/ (01.05.2019.)

15 The Regulation, Art. 6

[16] Voigt, P., Von dem Busche, A.: *"The EU General Data Protection Regulation, A Practical Guide", page 158. Springer, Cham, Switzerland, 2017.: "...this provision can be seen as a sweeping clause, as it grants a right to erasure where processing is unlawful, whether it is for a lacking legal permission for processing or for non-compliance with the Regulation, such as regarding the organisational obligations of the controller."*

- if it concerns the data processing relating to the offer of information society services directly to a child[17]

In the modern society there are numerous social networks and Internet services which are accessible practically to everyone, including all ages and social groups. These bring multiple benefits to a wide range of people. For inexperienced people there are risks in use of new technologies and services. The persons who use the information services have different goals, including the criminal activities (child pornography, computer deceptions, stealing of personal data, etc.). During the use of the Internet services, the users distribute their personal data to the providers of the services of the information society. However, if the user of the services, for instance, decides not to be present in a certain social network, he/she has the right to the erasure of the personal data ("the right to be forgotten").

3. CHALLENGES IN APPLYING THE REGULATION

It is in this area that significant problems arise as the Regulation can be difficult to apply. Identifying personally identifiable information can be difficult. Unstructured material such as e mails as it spreads beyond central stored information and can sit on cloud services. Managing the data can be problematic, it can be distributed across lots of applications and hosted on different hardware. This is particularly so in large Public sector organisations that have more than one silo. The enforcement can be expensive in legal fees for an individual especially if they are taking action in more than one country. The data may be stored on back-ups, a data carrier or in cloud storage, which is nearly impossible to prevent. The individual has to know (and be able to prove) that the company has his personal data stored. It is difficult and costly to obtain such proof, as that would require proceedings to obtain a court order for obtaining evidence (Tjin Tai 2016). Tai feels that for the right to be forgotten this barrier may be too high for ordinary individuals and may prohibit action in precisely the kinds of cases that the proposed right is intended to cover.

Children are specially protected from possible risks. Namely, they belong to an especially vulnerable group because of their age and inexperience and are generally not fully aware of the possible consequences during the use of the certain services of the information society, while on the other side the restriction of access to the children to such content is also questionable and practically unfeasible. Therefore, the Regulation determines that the consent to his/her personal data cannot be given by a child who is under the age of sixteen, and exceptionally under the age of thirteen (depending on the laws of the member state of the EU). In order to ensure the consent of the child who is under the minimum age, it is necessary to obtain the consent of the parent or the holder of the parental responsibility, regardless to the extent to which it is given.[18]

[17] The Regulation, Art. 17 (1 a-f)
[18] Ibid., Art. 8

Despite the fact that the data subject gave his consent as a child, he/she has the right to its' withdrawal as adult, too, and the controller must respect it.

The basic problem here is - how to recognize a child in the system? The Regulation is not specific in this area, since in the article 8 paragraph 2 of the Regulation states the following: "The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology." Therefore, the assessment about what the reasonable efforts are is up to the controller and additionally, in article 8 paragraph 3, the member states of the European Union are free to set the rules on the validity and the terms of making an agreement.[19]

The main problem considering the implementation of the right to erasure represents the erasure of data which has previously been published publicly, especially in the sphere of the Internet. Therefore, the implementation of such measures considers the accessible technology and the related costs during the procedure of deletion of all links, copies or reconstruction of the disputed personal data, which means that it is not possible to put unrealistic demands on the controller.[20]

4. THE RELATION BETWEEN THE RIGHT TO ERASURE OF THE DATA AND THE RIGHT TO ACCESS THE INFORMATION

The right to access the information in Republic of Croatia is defined as the fundamental human right by the provision of the Constitution which confirms the right to access the information which is held in the dominion of the public administrative bodies. The restriction to the consumption of that right must be proportional to the nature of the need for restriction in a concrete case, necessary in a free and democratic society and regulated by the law.[21] Hence, although the right to access the information is not absolute, the deprivation of the right to access the information is not an arbitrary matter and it must comply with the law regulations. Apart from the Constitution, the right to access the information is determined by the European Convention on the Human Rights, Convention on Access to Official Documents and the Law on the Right to Access the Information (hereinafter: LRAI).[22]

---

[19] Ibid., Art. 8 (3).: *"Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child."*

[20] Ibid., Art. 17 (2).: „*Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."*

[21] The Consitution of the Republic of Croatia. The Official Gazette of the Republic of Croatia 56/90., 135/97., 08/98., 113/00., 124/00., 28/01., 41/01., 55/01., 76/10., 85/10., 05/14., Article 38

[22] Law on the Right to Access the Information. The Official Gazette of the Republic of Croatia 25/13., 85/15.

The restriction of the right to access the information is exercised under article 1 of LRAI, which says that the provisions of LRAI cannot be applied to the court, administrative and other procedures, the information from the scope of the national intelligence system because of their secrecy and the classified data from the scope institutions. Besides that, article 15 LRAI says that the bodies of the public administration can restrict the access to the information in case if it refers to the information that is protected by the law from the sphere of the personal data protection.

In other words, organisational attempts to restrict the subjects' rights can only be pursued in cases when it is absolutely necessary and only in specific cases which are delineated by law.

The right to access information has a significant role in the development of the democratic society, because it represents the controlling mechanism that supervises the work of the institutions and enhances their transparency. Therefore, public administration bodies are obliged to publish data from the scope of their work on their own in order to make them accessible to interested parties and they must appoint a designated point of contact. His/her duty is to communicate with the public and harmonize the work of the institution with the relevant provisions of the law. It must be stressed that the information an individual has obtained can be used voluntarily, in commercial or non-commercial purposes.

In order to respect the right to access the information, the Regulations determine that the rules on personal data protection (including erasure) cannot be applied when it is necessary for exercising the right of freedom of expression and information; for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; for reasons of public interest in the area of public health, scientific/historical research etc. "[23][24][25]

[23] The Article 9 Paragraph 1 of the Regulation prohibits processing of the special categories of the personal data which refer to the "...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." Exceptionally this kind of data can be processed if, in accordance to the Art. 9 Paragraph 2 h) and i), when the *"...processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards. and in cases when "processing is necessary 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."* The data processing must be carried out in this case by the expert subject or under his supervision.

[24] The Regulation, Article 89 Paragraph 1 refers to the safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In case of this kind of processing it is necessary to apply certain technical and organizational measures (which are not enumerated in the text of the Regulation), but it is stressed out that during the application of such a measures it is necessary to respect **the principle of the minimisation of the data** and the **pseudonomysation** (data anonymisation).

[25] Ibid., Art. 17. Paragraph 3

In the case of a conflict between the right to information and the right to the erasure of the data, it is necessary to formally consider proportionality.[26] A proportionality test underpins decisions surrounding access or erasure of the data. The situation is not always black and white, therefore it is sometimes difficult to define the predominance of one of these rights and this is why it ends up in court procedures. The unequal jurisprudence can be stressed as the main problem in this area. It causes problems in the application of the relevant laws and produces legal uncertainty. As a consequence, it can lead to the censorship and erosion of the freedom of the media. For instance, it imposes the question whether a public person, such as a politician, entrepreneur or artist has the right to the same level of privacy as all other citizens. Then in turn it determines the level of privacy diminished by his/her public/online persona or appearances/conduct? How should the members of his/her family and the persons who are close to him/her be treated? Therefore, in the future it will probably be necessary to enhance legislation concerning the relationship between these two competing rights.

5. THE SIMILARITIES AND THE DIFFERENCES BETWEEN THE RIGHT TO REHABILITATION IN THE PENAL LAW AND THE RIGHT TO THE ERASURE OF THE DATA

According to the article 18 of the Law on Legal Consequences of the Sentence, Criminal Records and Rehabilitation (hereinafter: LLCSCRR) the right to rehabilitation means that "The perpetrator 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 the persons who did not commit a crime."[27] Thereafter the provisions of the LLCSCRR precise in which periods the right to rehabilitation comes into force under the condition that the perpetrator of the crime is not convicted again for another crime in the meantime.[28] "After the expiration of the periods which are determined in the paragraph 4

[26] LRAI, Art. 5 Paragraph 7: *„The test of proportionality of the public interest is the assessment of the proportionality between the reasons to access the information and the reasons to the limitation of the access; and giving the free access to the information if the public interest prevails."*

[27] Law on Legal Consequences of the Sentence, Criminal Records and Rehabilitation. The Official Gazette of the Republic of Croatia 143/12., 105/15., 32/17.

[28] Ibid., Art. 19. Paragraph 4: *„If the perpetrator of the crime has not been convicted in the meantime for another crime, the rehabilitation comes into effect by the force of law after the expiration of the following periods: twenty years from the day of after serving the sentence, limitation period or forgiven penalty in case of the conviction to long-term imprisonment; fifteen years after serving the sentence, limitation period or forgiven penalty in case of the conviction to ten years of imprisonment or more; ten years after serving the sentence, limitation period or forgiven penalty in case of the conviction to three years of imprisonment or more; five years after serving the sentence, limitation period or forgiven penalty in case of the conviction to one year of prison or more; five years from the day of serving the sentence, limitation period or forgiven penalty in case of the conviction to one year of prison or more and after the juvenile detention; three years from the day of serving, the limitation period or the forgiven penalty in case of the conviction to*

of this article the perpetrator of the crime is being considered as a non-convicted person and each use of his/her data as a perpetrator 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."[29]

The Ministry of Justice is legally responsible for decisions concerning rehabilitation.[30] In effect, this means that the right to rehabilitation is a right to the erasure of the data. The convicted person who committed a crime and served his/her sentence, should, after a certain period, have the opportunity to have his/her criminal past expunged. After the erasure of his/her personal data from the criminal records, the person who obtained the decision on rehabilitation can justifiably demand the removal of this data from his/her record.

Nevertheless, the right to erasure does not only refer to perpetrators of crime exclusively, but to the entire population. Also, the availing of the right to erasure is not conditional upon time limits and is at the request of individual data subject.

This provides an opportunity for a new start, without the burdens of the past. It is concerned with ensuring accurate in the interests of the data subject. The Regulation states that the information published must be necessary and proportionate.

6. CONCLUSION

The Regulations represent a huge step forward regarding the protection of the personal data in contemporary society that drastically changed comparing to a few decades ago due to the information technology revolution. Effectively, thanks to the real possibility of controlling the processing of his/her personal data nowadays, Namely, in the past personal data was physically separated and unreachable to a wide range of people, except officialdom. The Internet and social networks changed the lifestyle of the modern man and made personal data easily accessible to a huge spectrum of people. Organisations are very interested in certain data to use for their own purposes. Consequently, citizens have to have enhanced protection, which can (in certain cases) mean erasure.

The right to erasure of data must be balanced with the right to access the information. The absolute application of the right to erasure would potentially result in destruction of vital data protect citizens from undesirable and unlawful procedures. Therefore, in the near future we should continue with exploring the balance between these competing rights and needs of democratic societies and government institutions.

one year of prison, from the day of the payment of the money fine, from the day of the limitation period of the probation controls in case of the parole, from the day of completion of the work for the common good and from the day of the final judgement on release from the penalty."

[29] Ibid., Art. 19 (5)

[30] Ibid., Art. 20 (1)

There are many similarities in the rights concerning the rights to rehabilitation and the right to erasure. The rights to erasure are wider and easier to apply than those connected to rehabilitation, because its' implementation mainly depends on the will of the data subject. The rights to rehabilitation fall within the remit of the relevant institution. Looking to the future, an interesting area of research would be the interplay between these competing rights (given their different legal footing) and perhaps any future legal judgements on national and EU level.

The recent commencement of these provisions has presented challenges to all those involved. It will be interesting (in further research) to see how many subjects successfully avail other rights under the provisions. Only time will tell how the provisions and finer legal procedural points will develop. It is clear however that data subjects required and deserve the very best data protection (subject to legitimate, lawful and proportionate business needs of the state and other organisations).

BIBLIOGRAPHY:

1. Croatian Encyclopaedia. European Community for Coal and Steel. Zagreb. Leksikografski zavod Miroslav Krleža. Accessible: http://www.enciklopedija.hr/natuknica.aspx?id=18660 (21.2.2021.)
2. Europa.EU. Court of Justice of the European Union. URL: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_hr (24.3.2021.)
3. European Commission. Guidelines on consent under Regulation 2016/679 (wp259rev.01). URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (10.8.2021.)
4. 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 (12.4.2021.)
5. 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 (5.1.2021.)
6. EUR-Lex. Right to be forgotten on the Internet. URL: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=LEGISSUM%3A310401_1 (29.04.2021.)
7. Gonzalez Fuster, G:„The Emergence of Personal Data Protection as a Fundamental Right in the EU“. Page 259. Springer. Cham. Switzerland. 2014.
8. Information Commissioner's Office. Consent. URL: .https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (10.8.2020.)

9. 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/ (1.5.2020.)
10. Personal Data Protection Agency of the Republic of Croatia. About the Personal Data Protection Agency. URL: https://azop.hr/info-servis/detaljnije/o-agenciji-za-zastitu-osobnih-podataka (21.10.2020.)
11. Personal Data Protection Agency. The Guide through the General Data Protection Regulation. URL: https://azop.hr/info-servis/detaljnije/vodic-kroz-opcu-uredbu-o-zastiti-podataka (12.4.2021.)
12. T.F.E. Tjong Tjin Tai The Right to be forgotten. (2016) International Review of Law, Computers & Technology .Volume 30, 2016 - Issue 1-2 URL: https://www.tandfonline.com/author/Tjong+Tjin+Tai%2C+TFE (12.4.2021.)
13. Voigt, P., Von dem Busche, A.:"The EU General Data Protection Regulation, A Practical Guide", page 158. Springer, Cham, Switzerland, 2017.

Legislation and regulations

1. Directive 95/46/EU of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data EU. Regulations, Directives and other acts. URL: https://europa.eu/european-union/eu-law/legal-acts_hr (4.4.2021.)
2. 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 (29.10.2020.)
3. Law on Personal Data Protection. The Official Gazette of the Republic of Croatia 103/03., 118/06., 41/08., 130/11., 106/12.
4. Law on the Right to Access the Information. The Official Gazette of the Republic of Croatia 25/13., 85/15.
5. Law on Legal Consequences of the Sentence, Criminal Records and Rehabilitation. The Official Gazette of the Republic of Croatia 143/12., 105/15., 32/17.
6. Constitution of the Republic of Croatia. The Official Gazette of the Republic of Croatia 56/90., 135/97., 08/98., 113/00., 124/00., 28/01., 41/01., 55/01., 76/10., 85/10., 05/14.
7. 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 dana and on the free movement of such dana, and repealing Directive 95/46/EC (General Data Protection Regulation). URL:https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 (29.10.2020.)