*VARSTVOSLOVJE*
*Journal of Criminal Justice and Security*
*year 2023*
*volume 25*
*pp. 1–17*

# The Policing Perspective of Personal Data Protection and the Right to be Forgotten in Europe and in the Republic of Slovenia

**Miha Dvojmoč, Tinkara Bulovec, Katja Eman**

**Purpose:**

The article raises the question, whether the data protection regulation in police procedures is sufficient and whether it does not 'harm' the person subject to the procedure.

**Design/Methods/Approach:**

The impact, advantages and disadvantages of legislative changes on implementing specific police tasks (e.g. biometric data, facial recognition systems and automatic identification of vehicle registration plates) are presented, emphasising regulation in the Republic of Slovenia as a systematic literature review.

**Findings:**

The latest changes in personal data protection were related to the definition, collection, processing, use, transmission and storage of personal data. An individual has rights relating to access to information, processing, correction, restrictions on use, transferability, deletion and objection to the processing of personal data. When police operate within the law, their powers must align with constitutional and legal provisions. This alignment safeguards interventions in individual privacy. Yet, without legal clarity, known as *lex certa*, there's a risk of actions becoming unwarranted intrusions into rights and freedoms. A consensus is needed between the protection of individual privacy and enabling the effective investigation and control of crime by law enforcement authorities.

**Research Limitation/Implications:**

The research was focus only on data protection regulation in police procedures.

**Practical Implication:**

The findings of the article offer insight into data protection regulation in police procedures and highlights the gaps and formulate starting points for future research.

**Originality/Value:**

The article is the first systematic literature review in data protection in police procedures in Slovenia.

**Keywords**: protection of personal data, GDPR, police procedures, right to be forgotten, Slovenia

**UDC: 342.7:351.741(497.4)**

## Policijski vidik varstva osebnih podatkov in pravica do pozabe v Evropi in Sloveniji

**Namen:**

Članek zastavlja vprašanje, ali je ureditev varstva podatkov v policijskih postopkih zadostna in ali ne »škodi« subjektu postopka.

**Metode:**

V obliki sistematičnega pregleda literature so predstavljeni vplivi, prednosti in slabosti zakonskih sprememb na izvajanje policijskih nalog (npr. biometrični podatki, sistemi za prepoznavanje obrazov in avtomatska identifikacija registrskih tablic vozil) s poudarkom na ureditvi v Republiki Sloveniji.

**Ugotovitve:**

Zadnje spremembe na področju varstva osebnih podatkov se navezujejo predvsem na opredelitev, zbiranje, obdelavo, uporabo, posredovanje in shranjevanje osebnih podatkov. Posameznik ima pravice v zvezi z dostopom do informacij, obdelavo, popravkom, omejitvijo uporabe, prenosljivostjo, izbrisom ter ugovorom obdelave osebnih podatkov tudi v samih policijskih postopkih. Kadar policija deluje v okviru zakona, morajo biti njena pooblastila usklajena z ustavnimi in zakonskimi določili. Ta uskladitev ščiti posege v zasebnost posameznika. Vendar brez pravne jasnosti, znane kot *lex certa*, obstaja tveganje, da dejanja postanejo neupravičeni posegi v pravice in svoboščine. Potreben je konsenz med varstvom posameznikove zasebnosti in omogočanjem učinkovitega preiskovanja ter nadzora kriminalitete s strani organov kazenskega pregona.

**Omejitve:**

Članek je osredotočen le na ureditev varstva zasebnosti in podatkov v policijskih postopkih.

**Praktična uporabnost:**

Ugotovitve članka ponujajo vpogled v ureditev varstva podatkov v policijskih postopkih in osvetljujejo vrzeli ter oblikujejo izhodišča za prihodnje raziskave.

**Izvirnost/pomembnost prispevka:**

Članek je prvi sistematični pregled varstva osebnih podatkov v policijskih postopkih v Sloveniji.

**Ključne besede**: varstvo osebnih podatkov, GDPR, policijski postopki, pravica do

pozabe, Slovenija
**UDK: 342.7:351.741(497.4)**

## 1 INTRODUCTION

The protection of an individual's privacy and the related protection of personal data has been the subject of debate for some time. The development of advanced information and communication technology has allowed rapid and automatic processing of large amounts of data on the one hand. In contrast, an individual's personal data has become highly vulnerable and easily accessible to the general public, the state, and the private sector on the other hand. The fact that personal data may include sensitive information about an individual is one of the main reasons it should not be freely collected, used and transmitted. Its misuse could constitute a severe and criminal violation of an individual's privacy, a constitutionally protected right.

In general, the need to strike a balance between individuals' right to protect their personal data and the free economic initiative of corporations processing personal data has been growing in the last decade. The latter led to a high-profile European legislative package, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC – General Data Protection Regulation (hereinafter: "GDPR"), (2016). The "GDPR" which entered into force directly in the European Union's (hereinafter: EU) member states on 25 May 2018, is thus automatically applicable, becomes part of national law, and replaces possible conflicting provisions of national legislation. Thus, the field of personal data protection is subject to EU legislation if data is processed in one of the EU member states, regardless of the member state in which it is collected (Alessi, 2017).

The principle of data protection in the EU is not a new or foreign concept. However, recent developments and increasingly apparent shortcomings in the practical implementation of legislation have prompted the recent legislative reforms in police and criminal justice (Marquenie, 2017). As part of the extensive legislative package, the EU adopted "Directive (EU) 2016/680" of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data by competent authorities for prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (hereinafter: Directive (EU) 2016/680), 2016). Based on the "Directive (EU) 2016/680" (2016), the Republic of Slovenia adopted the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences ("Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD)", 2020).

The article is based on a qualitative analysis of literature and legislation in personal data protection at the EU level, with a case study of the Republic of Slovenia. Findings are supported with practice, which is regularly encountered by one of the co-authors working in data protection in the public sector. The purpose

of this article is to present the regulation and changes thereto in the field of personal data protection, with an emphasis on police procedures. In the article, the authors will highlight the issue of personal data protection in some areas of policing or the use of police powers, which include automated processing of personal data, with an emphasis on automated verification of motor vehicle license plates, use of biometric data and facial recognition technology. The institute of the right to forgotten will also be presented in the light of currently valid regulations, which under certain conditions allow the deletion, or forgetting, of personal data and contribute to personal data protection. Mentioned raises the question, whether this is sufficient and whether it does not 'harm' the person subject to the procedure.

## 2 REGULATION OF PERSONAL DATA PROTECTION

Information privacy or personal data protection is in the Republic of Slovenia derived from Article 38 of the Constitution of the Republic of Slovenia ("Ustava Republike Slovenije (URS)", 1991), which requires the lawful collection, processing, and use according to the purpose of collection. Paragraph 2 of the mentioned article states that the data subject is given the right to be informed of the collected data. In the event of misuse of personal data, the data subject has the right to judicial protection. The right to protect personal data or information privacy is not absolute but is by nature a relative right, meaning that it can be infringed under certain conditions. The Constitutional Court of the Republic of Slovenia (slov. *Ustavno sodišče Republike Slovenije*) allowed infringements following the principle of proportionality, besides the principle of legality. Later means the legal definition of the type of data that may be collected and processed, the purpose of their use, which must be constitutionally permissible, and the supervision over the collection, processing and use, not forgetting their confidentiality. Besides, "the right to privacy for an individual can end only when and where it collides with the legally demonstrated stronger interest of others" (Ustavno sodišče Republike Slovenije, 1997). In exceptional cases, public authorities can infringe on the right to privacy, which must be based on law and necessary to protect the higher interest. Higher interests are "state security, public security or economic well-being of the state in order to prevent disorder or a criminal offence, to protect health or morality, or to protect the rights and freedoms of other people" (Ustavno sodišče Republike Slovenije, 1997).

Personal data protection aims to protect the data subject and not the data itself. Resounding changes in personal data protection occurred with the implementation of the "GDPR" (2016), which introduced a new, broader definition of personal data.[1] The latter is defined in Article 4(1) of the "GDPR" (2016) as any information relating to a natural person (identified or identifiable) who can be identified, directly or indirectly, based on this data. Identifiers that identify a natural person in a specific way are "name, an identification number, location data, an online identifier[2] or to one or more factors specific to the physical, physiological, genetic,

1 *The definition of personal data, which is also used in Article 3(1) of "Directive (EU) 2016/680" (2016), is taken over from the "GDPR" (2016).*

2 *Online identifiers that may be associated with natural persons are „provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags" (Recital 30 of the "GDPR", 2016).*

mental, economic, cultural or social identity of that natural person". Recital 26 of the "GDPR" (2016) states that in determining the identifiability of a person "account should be taken of all the means reasonably likely to be used [...] either by the controller or by another person to identify the natural person".

With the adoption of the "GDPR" (2016), the position of the data subject has been further protected. Based on this, Chapter III of the "GDPR" (2016) details the rights of an individual about the processing and collection of their personal data. Marquenie (2017) points out that these rights are not absolute, but their exercise is subject to some limitations in protecting the integrity and confidentiality of criminal investigations and procedures. The fundamental rights granted to an individual under specific conditions based on the "GDPR"[3] are as follows the individual's right of access to information relating to the processing of their personal data; the individual's right to rectification and restrictions on the processing of their personal data; the individual's right to erasure or the right to forgotten; the right of the individual to the transferability of personal data and the right of the individual to object to the processing of personal data ("GDPR", 2016). EU or member state law to which the data controller or processor is subject may restrict by way of a legislative measure. The scope of the obligations and rights, in so far as its provisions correspond to the rights and obligations provided in this chapter, when such restriction respects the essence of the fundamental rights, freedoms, and represents a necessary and proportionate measure in a democratic society to safeguard the activities listed in Article 23 ("GDPR", 2016).

## 3 REGULATION OF PERSONAL DATA PROTECTION IN POLICE PROCEDURES

Police procedures are definitely among the procedures that represent the most significant violation of an individual's privacy and consequently require the highest legal regulation. In personal data protection during police procedures, the police constantly balance the successful execution of criminal procedures, public security and human rights. Appropriate powers are needed to enable law enforcement authorities to carry out their tasks, which may impact the right to protect personal data, so any infringement must be proportionate to the objective (Caruana, 2019). According to Kovač (2014), a (pre-trial) criminal procedure is the most critical, from infringement of the individual's rights. He adds that any infringements by state bodies of the individual's rights must be clearly defined by law, which is also provided for in Article 15 of the "URS" (1991) in the context of ensuring legal certainty. Such an arrangement provides individuals with the predictability of the conduct of state bodies and limits their arbitrary action, while any infringement of constitutional rights requires that we consider the principle of proportionality (Kovač, 2014).

Ensuring the highest level of protection of personal data of individuals and the effective exchange of personal data between competent authorities is crucial

3 *It is also worth mentioning that the last Eurobarometer on the topic of personal data protection (from 2019) showed that knowledge of the "GDPR" at the European and Slovenian level is low – only 31% of the population of the EU and 36% of Slovenes have heard of the "GDPR" and know what it is. Additionally, 35% (residents of EU countries and Slovenes) to 58% (Slovenes) or 59% of the population of EU countries do not know about individual's rights (European Commission, 2019).*

to ensure successful judicial and police activities in criminal matters, both at the national and international level. The latest European legislative package has also impacted policing, putting into practice "Directive (EU) 2016/680" (2016), protecting citizens' fundamental right to data protection in law enforcement authorities' use of personal data. The main objective of the abovementioned is to ensure that personal data on victims, witnesses and suspected offenders are appropriately protected. Besides, to facilitate cross-border cooperation in the fight against cross-border crime and terrorism in the EU (European Parliament, Fact Sheets on the European Union, 2019) by providing police and other law enforcement authorities in EU member states a more efficient sharing of information and data required for investigative procedures. The stated objective of "Directive (EU) 2016/680" (2016) is to ensure a consistent and high level of protection of natural persons concerning the processing of personal data and to facilitate free movement of personal data between competent authorities for the purposes set out in the directive (see Recitals 4 and 7).

The police tasks and powers sectoral law in Slovenia is the Police Tasks and Powers Act ("Zakon o nalogah in pooblastilih policije (ZNPPol)", 2013), containing provisions for collecting and processing personal data. The collection and processing of data are police powers that police officers may exercise in performing police tasks (Article 33). To perform police tasks, police officers may collect and process personal data, including biometric data of persons and other data (including data from confidential relationships and professional secrets) (paragraph 1 of Article 112). In practice, this is reflected in the fact that police officers conduct informational interviews and gather information directly from the person to whom such information refers or from other persons to whom they may provide such information.

The police may collect personal data from various databases and records. The "ZNPPol" (2013) also defines records and databases of personal data kept by the police, including their content, storage periods and blocking of data, and their handling after blocking (Articles 123–129 of the "ZNPPol", 2013). As part of the policing tasks related to proving minor offences or criminal acts and identification of perpetrators, checking the legality of exercising powers, monitoring public gatherings where minor offences and criminal acts can be expected, considering the circumstances, police officers may, under the principle of legality, use technical means for video and audio recording and "technical means for marking or identification of persons, vehicles and objects used in police" (Articles 113 and 114 of the "ZNPPol", 2013).

In November 2020, Slovenia adopted the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences ("ZVOPOKD", 2020), which governs the processing of personal data in connection with criminal offences and the related activity of administrative bodies with enforcement powers. The Act governs the protection of personal data processed by "the police, state prosecutor's offices, the Probation Administration of the Republic of Slovenia, Prison Administration of the Republic of Slovenia" and other statutory state bodies "responsible for the prevention, investigation, detection or prosecution of criminal offences or enforcement of criminal sanctions" (Article 1 of "ZVOPOKD",

2020). The Act stipulates for proper recording and monitoring of the use of the powers of competent authorities related to the collection of personal data. The Act sets out the legal basis for the processing of personal data, supervision by the Information Commissioner, minor offences, certain internal persons authorised for the protection of personal data, and exceptions to the protection of personal data. In the second chapter, the Act defines the rights of an individual regarding their personal data and the procedure before the competent authority. An individual thus has the right to obtain the information specified by law from the competent authority, to access personal data or obtain information whether their data is processed, obtain a copy or printout of such data, and correct, delete and restrict its processing. The competent authority provides these rights to the individual in a concise, comprehensible and accessible form. However, these rights are certainly not absolute. Expressly, they may be limited based on another law and may be exercised by an individual only in the manner and to the extent determined by another law. Furthermore, the right of an individual may also be partially or entirely restricted in order to prevent the influence or obstruction of official procedures, to ensure public security, security of the state or defence of the state, and to ensure the protection or exercise of human rights and fundamental freedoms of third parties ("ZVOPOKD", 2020).

Below, as an example of police procedures in which the police collect personal data for detecting, investigating or preventing criminal offences, and thus infringes on an individual's privacy, we cite automated processing of personal data, with an emphasis on automated verification of vehicle registration plates, use of biometric data and facial recognition system.

## 4 AUTOMATED PROCESSING OF PERSONAL DATA

Personal data processing is an overarching concept that means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 3(2) of "Directive (EU) 2016/680", 2016; Article 4(2) of the "GDPR", 2016). "Directive (EU) 2016/680" (2016) defines profiling in the same way as the "GDPR", specifically it "means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" (Article 3(4) of "Directive (EU) 2016/680", 2016; Article 4(4) of the "GDPR", 2016). Like Article 22 of the "GDPR" (2016), Article 11 (1) of "Directive (EU) 2016/680" (2016) also prohibits, in certain circumstances, decisions based solely on automated processing. Unlike Article 22 of the "GDPR" (2016), which states that the data subject has the right not to be the subject of a decision based solely on automated processing, Article 11 is designed as a prohibition. Later means that it is more reliable and protective than

the "GDPR". Lynskey (2019) concludes that what both articles have in common is that they have some limitations. Primarily, automated decision-making is allowed where permitted by EU or member state legislation. By adopting such legislation, member states can therefore justify fully automated law enforcement decision-making for systematic and/or individualised prediction of future offences. It is crucial that, according to Recital 38 of "Directive (EU) 2016/680" (2016), collection of personal data on an individual is not permitted by automated means alone, which have potentially detrimental legal effects or a significant impact on the individual. Article 11(3) of "Directive (EU) 2016/680" (2016) prohibits profiling that results in discrimination based on sensitive information.

In contrast to the "GDPR", which allows automated decision-making, if necessary for contractual purposes or based on the data subject's explicit consent, this is impossible under Article 11 of "Directive (EU) 2016/680" (2016) due to the existing imbalance of power between the data subject and the controller. The "GDPR" allows automated decision-making on a broader scale and provides a broader range of protective measures for individuals, which are defined, *inter alia*, in Recitals 67 and 68. They stipulate, for example, that further processing (which must also be clearly stated) and alteration must be prevented, the individual must be able to receive personal data concerning them in a specific form (when the basis is consent or contract), they must be able to transfer their data between data controllers ("GDPR", 2016).

"Directive (EU) 2016/680" allows for automated decision-making when EU or member state legislation permits, that such law ensures adequate protection of "the rights and freedoms of the data subject". Such a law must contain at least the right to "obtain human intervention on the part of the controller" (Article 11 of "Directive (EU) 2016/680", 2016).

## 4.1 Automated vehicle registration plate verification

The automatic processing of personal data and related protection of personal data has become apparent in the introduction of new police powers. In 2016, a proposed amendment to the Slovenian Police Tasks and Powers Act expressed staffing and technical limitations of the police. Consequently, a proposal was made to use an automatic system for verifying registration plates, which would pursue the public interest for greater security. The concern for protecting personal data in the case of automatic verification of motor vehicle registration plates took priority. The Decision of the Constitutional Court (Ustavno sodišče Republike Slovenije, 2019) states that "data on the registration plate (together with data on the date, place and time of recording)" would represent personal data of an identifiable individual (Article 4(1) of "GDPR", 2016; Article 3(1) of "Directive (EU) 2016/680", 2016). It states that "the data on the registration plate is intended to identify the individual and therefore represents personal data following the above definition" (Ustavno sodišče Republike Slovenije, 2019, p. 572). The envisaged possibility of automatic recording of registration plates and storage of data collected in this way in particular records for seven days was provided for in indent 22 of paragraph 1 of Article 128 of the Act Amending the Police Tasks and Powers Act ("Zakon o spremembah in

dopolnitvah Zakona o nalogah in pooblastilih policije (ZNPPol-A)", 2017). The Constitutional Court of the Republic of Slovenia (Ustavno sodišče Republike Slovenije, 2019) took the view that based on the article mentioned above, the police may not carry out the next step, automated comparison of "recorded and stored data with other personal data records". The current Article 112 of the "ZNPPol" (2013), which governs the collection of data, does not constitute a basis for such processing of personal data (Ustavno sodišče Republike Slovenije, 2019). Despite the possibility provided to the police by Article 122 of the "ZNPPol" (2013), it does not constitute a basis for automated processing of registration plates, "as this provision represents only restrictions on automated processing of personal data for police purposes and prohibits making personal profiles solely based on automated data processing" (Ustavno sodišče Republike Slovenije, 2019, p. 572). In rejecting the proposal for automated processing of registration plates by the police, the Constitutional Court relied on paragraph 2 of Article 38 of the "URS" (1991), which stipulates that the principle of legality be observed throughout the entire procedure of handling personal data. Similar was found by Woods (2017), who pointed out the importance of an individual's location privacy to the concept mentioned above of information privacy when using automated vehicle registration plate verification. Besides, in general, the use of automated vehicle registration plate verification remains problematic given the current legislation governing data collection. He then emphasises that the protection and use of data collected through automated vehicle registration plate checks are exposed to a legal challenge that has potentially far-reaching consequences.

## 4.2 Biometric data and the question of privacy

Hamann and Smith (2019) state that society and law enforcement authorities strive to keep up with modern technology that is expanding, evolving, and improving day by day. Technological innovations can also include biometrics, a possible way of establishing and verifying an individual's identity based on unique, permanent and inherent (physical, physiological and behavioural) characteristics (Informacijski pooblaščenec, n. d.). EU data protection rules clearly define the processing of biometric data. The "Directive (EU) 2016/680" and the "GDPR" define biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" (Article 4(14) of the "GDPR", 2016; Article 3(13) of "Directive (EU) 2016/680", 2016). Biometric data belongs to a particular type of personal data that are not allowed to be processed for "the purpose of uniquely identifying a natural person" (Article 9(1) of the "GDPR", 2016; Article 10 of "Directive (EU) 2016/680", 2016). Such data are, by their nature, always data that refers to a specific or at least identifiable person. Data on, for example, fingerprints always belong to a specific person (Informacijski pooblaščenec, n. d.). The Information Commissioner (Informacijski pooblaščenec, n. d.) states that an individual's biometric characteristics may fall into the category of sensitive data in cases where their use may identify specific types of sensitive

data that, except in exceptional cases, may not be collected (more details in Article 9(1) of the "GDPR", 2016; and Article 10 of "Directive (EU) 2016/680", 2016).

The Information Commissioner (Informacijski pooblaščenec, n. d.) points out that the definition of biometric measures includes two identification procedures – identification and identity verification. Paragraph 1 of Article 112 of the "ZNPPol" (2013) describes biometric characteristics in detecting and investigating criminal offences. The identification procedure may be carried out by police officers in cases when "it is necessary and required to compare fingerprints and palm prints, photographs with photographs of other persons, and compare DNA profiles because of the circumstances of a specific criminal offence." In these situations, automatic processing of these characteristics can be used. In Part II of the draft legislation Personal Data Protection Act ("Predlog Zakona o varstvu osebnih podatkov (ZVOP-2)", 2021), the provisions on video surveillance on biometrics have been partially revised, among other things. Personal data processing using biometrics is limited in Article 78 of the proposed act and can only be determined by law, which, among other things, also defines the conditions for their use and the restriction of use ("Predlog Zakona o varstvu osebnih podatkov (ZVOP-2)", 2021).

## 4.3 Facial recognition systems

In recent years, we have seen an increase in the use, storage and dissemination of facial photographs in the private and public sectors. Mentioned, with the development of technology – applications and artificial intelligence – and concern for protecting individuals' privacy led to the response of legislators. In the previous subchapter, we discussed that particular concerns and risks had been considered at the legislative level in connection with the processing of biometric data, including faces. The use of facial recognition systems, therefore, infringes on the sphere of personal data of a specific type, the collection of which is permitted provided there is the explicit consent of the data subject and in cases where processing is necessary for reasons of public interest (details in Article 9(1) of the "GDPR", 2016; and Article 10 of "Directive (EU) 2016/680", 2016). For automated comparison of photographs, the Slovenian police may use the Face Trace automatic face recognition system, which has recently been the subject of multiple supervision by the Information Commissioner (Prelesnik, 2021). According to paragraph 2 of Article 149 of the Criminal Procedure Act ("Zakon o kazenskem postopku (ZKP-UPB8)", 2021), the police may "[…] photograph a person for whom there are grounds for suspecting that they have committed a criminal offence […]", and the photographs are in this case stored in the records of photographed persons (Article 123 of the "ZNPPol", 2013). During the inspection procedure, which involved a comprehensive assessment of the lawfulness of personal data processing within the Registry, the Information Commissioner found no systemic irregularities. However, it is crucial to recognize that the absence of such irregularities does not eliminate the potential for the misuse of the Face Trace module in practical applications, despite existing safeguards. This includes the module being used in a manner or for purposes that violate

legal prescriptions. In 2021, the Information Commissioner received information and reports indicating suspicions of the Police possibly using automated photo comparison to identify participants in various rallies in Slovenia, suggesting the potential for an illicit deployment of the Face Trace module (Prelesnik, 2021).

Facial recognition technology addresses many modern needs for the identification and verification of personal data. The automated biometric system operates based on pattern recognition. Introna and Nissenbaum (2010) add that the process of facial recognition is a typical task of identification, which should not be performed without respecting the principles of privacy, justice, freedom, independence and security. The Slovenian police may use photographs from these records for automatic face recognition in the said programme, the use of which is permitted in cases of detection and investigation of criminal offences or when this is necessary and required because of the circumstances of the act (Prelesnik, 2021; Article 112 of the "ZNPPol", 2013). The perpetrator's photo is entered into the module, which is not connected to a network outside the police system, based on a photo-robot or snapshot. The module performs an automatic comparison with the records. The final identification is not only the result of an automated comparison but is also preceded by manual comparison of facial features. The system has mechanisms in place to prevent the possibility of misuse and to provide for the option of subsequent audit and verification of the legality of personal data processing (Prelesnik, 2021).

Purshouse and Campbell (2019) point to reasons that, despite the accuracy of the technology and the benefits it brings for detection and investigation, should be considered and constitute grounds for limiting the use of this technology. Like Introna and Nissenbaum (2010), Purshouse and Campbell (2019) point out that limiting technology is necessary due to its infringement of all individuals' human rights in a specific public space at a specific time. Purshouse and Campbell (2019) add that the principle of necessity suggests the need for a selective approach to the use of facial recognition technology in public spaces. The use of such technology, in their view, should be a response to detected, credible and severe threats to public security. Furthermore, they highlight transparency and accountability in police use of facial recognition technology (Purshouse & Campbell, 2019). In addition to the vital element of necessity, the use of said technology must also meet the requirements of proportionality, meaning that the infringement of the right to protection of personal data must outweigh the right to protection of personal data (Bu, 2021).

The "GDPR" generally prohibits the processing of biometric data for unique identification, except in the case of one of the ten exceptions (Article 9(2) of the "GDPR", 2016). National and EU legislators have the discretion to decide in cases where the use of this technology provides proportionate and urgent infringement of human rights (Article 9(2)(g) of the "GDPR", 2016). The use of automatic facial recognition by law enforcement agencies is not subject to the "GDPR" (2016) but to "Directive (EU) 2016/680" (2016). Petersen (2019) expressed concern that, despite the "GDPR", almost all European countries have regulations governing data protection and privacy concerning biometrics, particularly the consent required for their storage and use. He points out that in the context of biometric data, further

clarification is needed on specific issues related to the very meaning of biometric processing, the issue of consent for identification rather than authentication, and which legal framework needs to be considered.

The "GDPR" raises questions about the legality of new storage methods and mechanisms for transferring biometric data. Khan (2019) states that many societal challenges posed by automatic facial recognition are not fully addressed in the "GDPR". Mentioned is attributed mainly to non-updated conceptual and theoretical challenges. Bu (2021) points to the lack of well-defined regulations that would regulate the collection, use, dissemination and storage of biometric identifiers, which has led to ethical and legal complications in practice. The use of facial recognition technology should have an appropriate legal basis, and it should follow the principles of necessity, proportionality and justification. It is essential to reach a consensus on privacy protection while allowing law enforcement agencies to use exceptional tools to investigate and control crime.

## 5 RIGHT TO BE FORGOTTEN

The right to be forgotten represents a relatively new concept that in today's digital world, within the framework of the right to privacy, recognises the individual's right to control how their personal data appear and are stored. The purpose of the right is to find a balance between the individual's right to privacy and the public's right to information (Stenning, 2016). The right to be forgotten is defined in the "GDPR" (2016), "Directive (EU) 2016/680" (2016), and the "ZVOPOKD" (2020).

Article 17 of the "GDPR" (2016) defines the right to erasure ("right to be forgotten") in a way that grants an individual the right to have their personal data erased, while the controller's obligation is to erase such data without undue delay, in cases where 1) "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed"; 2) "the data subject withdraws consent on which the processing is based[4]" and "where there is no other legal ground for the processing"; 3) "the data subject objects to the processing pursuant to Article 21(1)[5] and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)[6]"; 4) "the personal data have been unlawfully processed"; 5) "the personal data have to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject"; 6) "the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)[7]". According to paragraph 3 of Article 17 and Recital 65 of the "GDPR"

4 *Consent to the processing of personal data is defined in the first points of Article 6(1) and Article 9(2) of "GDPR"(2016).*

5 *The right to object to the processing of personal data based on Article 6(1)(e), the controller processes personal data in the public interest or in the exercise of public authority, or of Article 6(1)(f), processing for legitimate interests, with the exception where the fundamental rights and freedoms of the individual prevail, especially when personal data refers to a child. In these cases, the controller must prove legitimate grounds for further processing, which must compellingly override the individual's „interests, rights and freedoms" (Article 21(1) of "GDPR", 2016).*

6 *The right to object in cases of processing of personal data for the purposes of direct marketing (Article 21(2) of "GDPR", 2016).*

7 *„Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given*

(2016), the right to be forgotten or erasure an individual's personal data is not absolute. Exceptions are defined in Article 17(3) of the "GDPR" (2016), which states that erasure is not possible in the following cases: 1) "for exercising the right of freedom of expression and information"; 2) for performing a legal obligation of processing, for performing a task carried out in the public interest or by an official authority; 3) for the public interest; 4) archiving (in the public interest, scientific or historical research purposes or statistical purposes); and 5) when erasure prevents "establishment, exercise or defence of legal claims".

Article 16 of "Directive (EU) 2016/680" (2016) defines the right to rectification or erasure of personal data and the restriction of their processing explicitly. The data subject has the right to request that the controller corrects their personal data if inaccurate. Considering the purpose of processing, an individual has "the right to have incomplete personal data completed, including by means of providing a supplementary statement". In cases where individuals dispute the accuracy of their personal data and their accuracy cannot be verified, and in cases where the retention of personal data is necessary for evidence, the controller has the option to waive the erasure and restrict processing instead.

At the end of 2020, the provisions of "Directive (EU) 2016/680" (2016) were transposed into the Slovenian Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences ("ZVOPOKD", 2020). It stipulates that when the collected personal data relates to a specific individual, the individual is entitled to request the erasure of personal data according to Article 26 of the "ZVOPOKD" (2020). The data subject may exercise the right to erasure with the controller of any personal data collection or record, including the police. The right is granted to the individual in cases of violation of the principle of personal data protection (Article 5), the legality of processing (Article 6) or legality of the processing of special categories of personal data (Article 7), and in cases when personal data must be erased to fulfil the legal obligation of the competent authority. Erasure of personal data may be refused, or the competent authority may order a restriction on processing, in cases where: 1) "the data subject disputes the accuracy or up-to-dateness of personal data and the accuracy or up-to-dateness cannot be verified" or 2) "retention of personal data must continue for the purpose of evidence" (Article 26) ("ZVOPOKD", 2020).

As mentioned in the introduction, we cannot ignore whether the various data collection procedures do not 'harm' the person subject to the procedure. Another question also arises: Is the erasure of the personal data collected, which is made possible by the right to be forgotten, good or bad? It is most likely positive from the individual's point of view and negative from the point of view of law enforcement agencies. The issue occurs because this subject matter is still new and unresolved, with very little case law, and the 'misuse' of the institute for personal purposes can also occur quickly. The abovementioned has already been pointed out by the previous Slovenian Information Commissioner (Pirc Musar, n. d.). Besides, Kučić (2014) noted that unofficial analysis of the first 12,000 requests for erasure showed that concerns were justified. "Among the users of Google's online form, most (almost a third) were accused of fraud by Google's search results. Approximately a fifth of the applicants wanted to hide past violent or criminal acts. A good tenth

*or authorised by the holder of parental responsibility over the child" (Article 8(1) of"GDPR", 2016).*

had been arrested for child pornography, and the applicants also included corrupt politicians, penalised physicians and convicted paedophiles. This information was immediately seized by American commentators and used to prove that the right to be forgotten electronically should not prevail over the right to information and that European regulators should leave the Internet – and their Internet companies – alone" (Kučić, 2014). Meanwhile, we do not (yet) have information about the misuse of the institute by the police.

## 6 CONCLUSION

The technology has overtaken the existing legal basis, raising concerns about personal data protection. Illegal use of specific methods, e.g. facial recognition combined with checking social media posts, can lead to a state of complete control. Privacy and protection of personal data, which constitute a constitutionally protected right, consequently require a statutory definition of interventions, reflecting the legality principle. Appropriate data protection standards in the field of law enforcement and criminal justice are beneficial for all stakeholders involved, as they protect fundamental human rights of the general public while improving international cooperation, increasing the efficiency of law enforcement, and strengthening public confidence in them (Marquenie, 2017).

Recital 19 of the "GDPR" (2016) states that the protection of individuals concerning the processing of personal data by the competent authorities to prevent, investigate, detecting or prosecuting criminal offences or enforcing criminal sanctions, including protection against threats to public security and their prevention, and free flow of such data, is regulated by a specific EU legal act – the "Directive (EU) 2016/680" (2016). The main objective of the Directive is to ensure that personal data on victims, witnesses and suspected offenders are adequately protected and facilitate cross-border cooperation in the fight against cross-border crime and terrorism (European Parliament, Fact Sheets on the European Union, 2019). The data collected by law enforcement authorities must be processed only for these purposes, and above all, must be processed lawfully and fairly and collected for specified, explicit and legitimate purposes. The data must be accurate, relevant and not excessive concerning the purpose for which it is processed. The data must also be appropriately protected, including protection against unauthorised or unlawful processing. The data is kept in a format that allows identification only for the period necessary for processing.

Caruana (2019) identifies some critical points related to "Directive (EU) 2016/680" (2016) and the "GDPR" (2016), stemming mainly from the complex demarcation between "Directive (EU) 2016/680" (2016) and the "GDPR" (2016), supervision and enforcement, in particular the supervision by independent supervisory authorities and the transfer of data at an international level, as well as other beneficiaries. He pointed out a noticeable inconsistency between "Directive EU 680/2016" and the "GDPR", supporting this claim with the case of the distinction between the powers of independent supervisory authorities and the absence of a compliance mechanism in the "Directive EU 680/2016". He points out that the assessment of whether a fair and effective balance between the sometimes

conflicting data protection forces on the one hand and law enforcement and public security requirements, on the other hand, will depend on the application of legislation, its transposition into the practice of EU member states, and future reforms (Caruana, 2019). Additional legal changes are as well expected in Slovenia in the field of personal data protection. The proposal of the new Personal Data Protection Act envisages the regulation of the field of personal data protection in three systemic regulations – directly applicable provisions of the "GDPR", the new personal data protection act and "ZVOPOKD" ("Predlog Zakona o varstvu osebnih podatkov (ZVOP-2)", 2021).

The presented article shows a theoretical insight into data protection concerning police procedures. Some advantages and disadvantages of the current regulation of specific police procedures were pointed out, which should be supported by empirical research of police practice. Further research will also be needed in implementing innovations or improvements in personal data protection and their impact on ensuring the protection of individual and human rights, public security, and execution of criminal procedures.

## REFERENCES

Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review, 32*(1), 145–171.

Bu, O. (2021). The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review, 2*, 113–145. https://doi.org/10.1365/s43439-021-00022-x

Caruana, M. M. (2019). The reform of the EU data protection framework in the context of the police and criminal justice sector: Harmonisation, scope, oversight and enforcement. *International Review of Law, Computers & Technology, 33*(3), 249–270. https://doi.org/10.1080/13600869.2017.1370224

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. [Directive (EU) 2016/680]. (2016). *Official Journal of the European Union*, L 119/89, 89–131.

European Commission. (2019). *Special Eurobarometer 487a: The general data protection regulation: Report*. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=69701

European Parliament, Fact Sheets on the European Union. (2019). *Personal data protection*. https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection

Hamann, K., & Smith, R. (2019). Facial recognition technology: Where will it take us?. *Criminal Justice, 34*(1), 9–13.

Informacijski pooblaščenec. (n. d.). *Ureditev biometrijskih ukrepov po ZVOP-2* [Registration of biometric measures according to ZVOP-2]. https://www.ip-rs.

si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/prijava-biometrijskih-ukrepov/

Introna, D. L., & Nissenbaum, H. (2010). *Facial recognition technology: A survey of policy and implementation issues.* https://eprints.lancs.ac.uk/id/eprint/49012/1/Document.pdf

Khan, M. (22. 8. 2019). EU plans sweeping regulation of facial recognition. *Financial Times*. https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9

Kovač, J. (2014). Razmerje med varnostjo in svobodo ter posegi v človekove pravice v kazenskopravnem pomenu [The relationship between security and freedom and interference with human rights in the sense of criminal law]. In B. Flander, I. Areh, & M. Modic (Eds.), *Zbornik prispevkov, 15. slovenski dnevi varstvoslovja.* Fakulteta za varnostne vede. https://www.fvv.um.si/dv2014/zbornik/Kovac.pdf

Kučić, L. J. (6. 6. 2014). Pravica do elektronske pozabe [The right to be forgotten in terms of electronic records]. *Delo*. https://old.delo.si/zgodbe/sobotnapriloga/pravica-do-elektronske-pozabe.html

Lynskey, O. (2019). Criminal justice profiling and EU data protection law: Precarious protection from predictive policing. *International Journal of Law in Context, 15*(2), 162–176. https://doi.org/10.1017/S1744552319000090

Marquenie, T. (2017). The police and criminal justice authorities directive: Data protection standards and impact on the legal framework. *Computer Law & Security Review, 33*(3), 324–340. https://doi.org/10.1016/j.clsr.2017.03.009

Petersen, J. (2019). The complexity of consent and privacy in biometrics – Worldwide. *Biometric Technology Today, 2019*(8), 5–7. https://doi.org/10.1016/S0969-4765(19)30113-4

Pirc Musar, N. (n. d.). *Pravica do pozabe in o svobodi laganja* [The right to be forgotten and the freedom of lying]. Pirc Musar & partnerji, odvetniška družba. https://pirc-musar.si/sl/pravica-do-pozabe/

Predlog Zakona o varstvu osebnih podatkov (ZVOP-2) (EVA: 2018-2030-0045) [Draft of the Personal Data Protection Act]. (2021). *Republika Slovenija eUprava.* https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/487030?disposition=inline

Prelesnik, M. (14. 4. 2021). *Policijski sistem Face Trace sicer temelji na biometrični obdelavi osebnih podatkov, a ne omogoča identifikacije* [The Face Trace police system is based on biometric processing of personal data, but does not allow identification]. Informacijski pooblaščenec. https://www.ip-rs.si/novice/policijski-sistem-face-trace-sicer-temelji-na-biometri%C4%8Dni-obdelavi-osebnih-podatkov-a-ne-omogo%C4%8Da-identifikacije

Purshouse, J., & Campbell, L. (2019). Privacy, crime control and police use of automated facial recognition technology. *Criminal Law Review, 2019*(3), 188–204.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC – General Data Protection Regulation [GDPR]. (2016). *Official Journal of the European Union*, L 119/1, 1–88.

Stenning, A. (2016). Gone but not forgotten: Recognizing the right to be forgotten in the U.S. to lessen the impacts of data breaches. *San Diego International Law Journal, 18*(1), 129–160.

Ustava Republike Slovenije (URS) [Constitution of the Republic of Slovenia]. (1991, 1997, 2000, 2003, 2004, 2006, 2016, 2021). *Uradni list RS,* (33/91-I, 42/97, 66/00, 24/03, 47/04, 68/04, 69/04, 68/06, 140/13, 143/13, 47/13, 47/13, 97/16, 99/16, 75/16, 92/21).

Ustavno sodišče Republike Slovenije. (1997). Odločba OdlUS VI, 158 z dne 27. 11. 1997.

Ustavno sodišče Republike Slovenije. (2019). Delna odločba o razveljavitvi četrtega odstavka 113. člena, 32. točke drugega odstavka 123. člena, 32. točke 125. člena in dvaindvajsete alineje prvega odstavka 128. člena Zakona o nalogah in pooblastilih policije [Partial decision on the repeal of paragraph 4 of Article 113, point 32 of paragraph 2 of Article 123, point 32 of Article 125 and indent 22 of paragraph 1 of Article 128 of the Police Tasks and Powers Act]. *Uradni list RS, 29*(46), 5717. https://www.uradni-list.si/_pdf/2019/Ur/u2019046.pdf

Woods, L. (2017). Automated number plate recognition: Data retention and the protection of privacy in public places. *Journal of Information Rights Policy and Practice, 2*(1). https://doi.org/10.21039/irpandp.v2i1.35

Zakon o kazenskem postopku (ZKP-UPB8) [Criminal Procedure Act]. (2021). *Uradni list RS,* (96/22, 2/23, 89/23).

Zakon o nalogah in pooblastilih policije (ZNPPol) [Police Tasks and Powers Act]. (2013, 2015, 2017, 2019, 2021). *Uradni list RS,* (15/13, 23/15, 10/17, 46/19, 47/19, 153/21).

Zakon o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije (ZNPPol-A) [Act Amending the Police Tasks and Powers Act]. (2017). *Uradni list RS,* (10/17).

Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD) [Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences]. (2020). *Uradni list RS*, (177/20).

## About the authors:

**Miha Dvojmoč,** Associate Professor, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia. E-mail: miha.dvojmoc@um.si

**Tinkara Bulovec,** MA, PhD student at Faculty of Criminal Justice and Security, coordinator at Municipal Constabulary Department, Municipality of Ljubljana, Ljubljana, Slovenia. E-mail: tinkara.bulovec@ljubljana.si

**Katja Eman**, Associate Professor, University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia. E-mail: katja.eman@um.si