Law Enforcement Directive Implementation Country Report: Slovenia

Primož Križnar

EDRi
European Digital Rights

Law Enforcement Directive Implementation
Country Report: Slovenia

Primož Križnar, 19 June 2024

TABLE OF CONTENTS

1. Introduction

On 27 April 2016, the European Parliament and the Council adopted Directive (EU) 2016/680 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 (hereafter "law enforcement purposes"), and on the free movement of such data, repealing Council Framework Decision 2008/977/JHA (hereinafter referred to as LED, or Law Enforcement Directive).

Slovenia was required to adopt and publish the laws and regulations necessary to comply with the LED by 6 May 2018. These regulations should thus have been in force from 6 May 2018, and should have included appropriate references to the LED (Article 63(1) and (2) of the LED). However, Slovenia only transposed the LED into its national legislation on 20 November 2020. On that day, it adopted the Personal Data Protection Act in the Field of Criminal Offences (ZVOPOKD),[1] which was published in the Official Gazette of the Republic of Slovenia on 1 December 2020, and came into force on 31 December 2020. Thus, Slovenia missed the deadline for transposing the LED into its legal order.

Upon reviewing the legal and subordinate regulations in Slovenia's legal system, no other legal acts implementing the LED could be found. The ZVOPOKD is also the only legal act that references the LED (Article 1(4) ZVOPOKD). According to desk research, all LED provisions have been transposed into the Slovenian legal order through the ZVOPOKD and are in conformity.

A review of case law in this area shows that the provisions of the ZVOPOKD have been used in three court decisions, and the Information Commissioner of the Republic of Slovenia (IPRS), the Slovenian Data Protection Authority, has issued several opinions related to them. Using the search parameters "ZVOPOKD" and "2016/680", four professional articles and three Master's theses mentioning the provisions of the ZVOPOKD and the LED can be found.

This research focuses on the main objectives of the study, which relate to the rights of individuals whose personal data is processed, the processing of special categories of personal data, the legal bases for the processing of personal data, and the impact of the legislation on the use of new artificial intelligence technologies in law enforcement.

2. Executive Summary

Despite Slovenia missed the deadline for transposing the LED into its legal framework, it was eventually transposed through the ZVOPOKD. Many provisions of this law are either directly copied or closely aligned with the wording of the LED. There are no issues regarding the scope of the LED, as the ZVOPOKD clearly defines both the concept of a competent authority (personal scope) and the notion of a criminal offense (material scope). The enforcement of the LED is entrusted to the IPRS, which also oversees the enforcement of the GDPR.

Time limits for the erasure of personal data or periodic reviews of the necessity to retain such data are regulated by sectoral laws, such as Article 128 of the ZNPPol, rather than the ZVOPOKD. Therefore, the general requirement under Article 5 of the LED is fulfilled.

The legal basis for data processing, as required by Article 8 of the LED, is also outlined in sectoral legislation. Given the same requirement in Article 38(2) of the Constitution, an exact legal basis is crucial when supervisory authorities or courts assess the legality of data processing. This is particularly important for processing special categories of personal data, which is generally

[1] For references to all laws cited in this report, see section 7.

prohibited, but exceptions under the LED allow processing under strict cumulative conditions outlined in Article 7(2) of the ZVOPOKD. Because these conditions must be met for the processing of special categories of personal data, the legal framework for processing sensitive personal data in Slovenia is more detailed and stricter than for non-sensitive data. If these conditions are not met, processing is prohibited.

Regarding automated decision-making, Slovenian law is aligned with the LED, requiring that such decisions are not based on special categories of personal data unless appropriate safeguards are in place. Profiling that leads to discrimination is also prohibited. National legislation also provides for appropriate safeguards to protect the rights and freedoms of data subjects in cases where automated decision-making is permitted by law.

Slovenia has opted to utilize the LED's provision to restrict data subjects' right of access to their personal data. The competent authority is not required to provide information if doing so would obstruct or compromise official procedures, particularly if it would reveal the identities of individuals under covert investigative measures. Furthermore, individuals' rights to access their personal data may be partially or entirely restricted if such limitations are necessary and proportionate for the prevention or detection of crime, public safety, state security or defense, or the protection of third parties' human rights and fundamental freedoms. These exemptions are clearly outlined in the ZVOPOKD, and data controllers have no discretion in their application.

Considering the scope of this report, the relevant national provisions are in compliance with the LED, and no legal gaps have been identified. Consequently, no further legislative action is required. However, it should be noted that these provisions are not frequently applied in practice by competent authorities, making it difficult to assess the practical implementation of the LED. Since the adoption of the ZVOPOKD, the IPRS has mainly issued non-binding legal opinions, and only a few court rulings are available—none of which apply the ZVOPOKD directly, but only indirectly. Careful consideration will be necessary when the legislature is drafting or amending laws related to big data analytics. Some technological solutions (GPS tracking, automated judicial decision-making, and facial recognition) lack a clear legal basis, while others (IMSI catchers and license plate recognition systems) have insufficient legal foundations. Otherwise, no specific recommendations are necessary.

3. General provisions

3.1 Applicability

The law through which the LED was transposed into the Slovenian legal order applies to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Article 1(1) ZVOPOKD).

Competent authorities are exhaustively listed in Article 1(1) ZVOPOKD and include the police, state prosecutors, the Probation Administration of the Republic of Slovenia, the Administration of the Republic of Slovenia for the Execution of Criminal Sanctions, and other state authorities of the Republic of Slovenia that are legally designated as competent for law enforcement (e.g. criminal courts, the Intelligence and Security Service, and the Office for Money Laundering Prevention).[1]

[1] These competent authorities are the data controllers (Article 4(7) ZVOPOKD), while natural or legal persons, other state authorities, local self-government authorities, public agencies, or other bodies that process personal data on behalf of the controller are processors (Article 4(8) ZVOPOKD).

When courts are deciding on criminal matters, provisions of the ZVOPOKD are used regarding the processing and access to personal data in criminal matters (Article 1(2) ZVOPOKD). Furthermore, ZVOPOKD regulates: (i) the conditions for the lawful and fair processing of personal data; (ii) procedures and methods for detecting and preventing unlawful interference with the rights of individuals to whom the personal data relate; (iii) the means of exercising their rights; and (iv) the transfer of personal data to third countries and international organisations (Article 1(3) ZVOPOKD).

The ZVOPOKD also applies to the processing of personal data that is wholly or partly carried out by automated means, and to the processing of personal data that is part of a collection or intended to form part of a collection that is not carried out by automated means (Article 3).

3.2 Supervisory authority

To effectively protect the legality and fairness of personal data processing, the ZVOPOKD stipulates the supervisory powers and measures that can be enacted by the supervisory authority, as well as liability for offences regarding their violations. It designates the Information Commissioner of the Republic of Slovenia (IPRS) as the supervisory authority (Article 75(1) ZVOPOKD). **The IPRS mostly issued non-binding legal opinions on cases pertaining to the application of ZVOPOKD, but it can also issue binding ones following inspections.**

If an individual suspects illegal processing of personal data, they can file a complaint with the IPRS for a breach of data protection. In such a case, the IPRS will investigate in order to determine if the data controller unlawfully processed the personal data. The complaint must therefore establish a reasonable suspicion of a data protection violation, which means it should specify, for example, when, in which procedures, with which specific actions, and which personal data were allegedly unlawfully processed by the controller.[2]

When a more specific regulation (*lex specialis*) governs the data processing, the IPRS is not competent. In this context, the IPRS has dealt with the following requests:

- A state prosecutor's office requested data about a specific commentator on a media portal. The IPRS decided that such requests fall under Article 149.c of the Criminal Procedure Act (ZKP, regulating police powers in criminal investigations), which states that the court is responsible for deciding whether the media company is permitted to disclose the personal data of a commentator to the state prosecutor's office.[3]
- A suspect wished to inspect material evidence held by the police after the district court had already denied his request. The IPRS declared itself not competent, stating that this matter falls within the jurisdiction of the court as part of the criminal procedure.[4]
- An individual requested the IPRS's opinion regarding hate speech in comments on a Slovenian online media platform. The IPRS concluded it was not competent to address issues related to the exercise of the right to freedom of expression and its limitations. The individual was directed to the Inspectorate of the Republic of Slovenia for Culture and Media (for moderation policies) or to the police and state prosecutor's office (if the comments potentially constitute the criminal offence of public incitement to hatred, violence or intolerance under Article 297 of the Criminal Code (KZ-1)).[5]
- A prison requested the legal evaluation of the establishment of video surveillance in the kitchen, dining room and warehouse areas by the IPRS. In this case the latter was competent, but it emphasised that the ZVOPOKD does not regulate this area. Rather,

[2] IPRS Opinion 07121-1/2023/391 from 5.4.2023.
[3] IPRS Opinion 07121-1/2023/1223 from 3.1.2024.
[4] IPRS Opinion 07121-1/2022/125 from 3.2.2022.
[5] IPRS Opinion 07121-1/2023/203 from 17.2.2023.

specialised laws (ZIKS-1 and ZVOP-2) constitute the legal basis for such surveillance measures, which the IPRS assessed in its opinion.[6]

4. Data subject rights

According to the ZVOPOKD, individuals can exercise their rights to obtain information, access data, as well as to correct, delete and restrict the processing of their personal data before the competent authority. They may also assert these rights with the processor if the competent authority entrusts the processing to a processor who independently determines other purposes or means of processing personal data contrary to the provisions of the ZVOPOKD or the concluded data processing agreement (Article 18(2) in conjunction with Article 44(5) ZVOPOKD). For matters concerning the procedure for exercising the rights of individuals whose personal data is being processed and for decision-making on these rights, the provisions of the General Administrative Procedure Act (ZUP) apply (Article 19 ZVOPOKD).

4.1 Communication with the competent authorities

The competent authority must provide individuals whose personal data is being processed with all information regarding the data processing and all communications related to the exercise of their rights in a concise, understandable and easily accessible form, and in clear and simple language. The competent authority may provide this information and communication to the individual in all appropriate ways, including electronically, and should generally provide it in the format in which the request was submitted (Article 21(1) ZVOPOKD).

The competent authority facilitates the exercise of individual rights, particularly by preparing forms[1] for the exercise of rights (Article 21(2) ZVOPOKD). Additionally, the competent authority provides the individual with the following (free of charge):[2]

a) all information about data processing and all communications related to exercising their rights;
b) in cases of automated data processing and profiling – a re-examination and manual review of the decision by a natural person and the ability to express their own views;
c) the exercise of individual rights;
d) notifications of personal data security breaches (Article 21(3) ZVOPOKD).

The competent authority immediately rejects an individual's request if it demonstrates that:

1) the request is obviously unfounded based on its content, or
2) the requests of the individual are excessive, especially because the individual unreasonably and repeatedly submits the same requests (Article 22 ZVOPOKD).[3]

4.2 Providing information

In accordance with Article 23 ZVOPOKD, each competent authority must make the following information available:[4]

[6] IPRS Opinion 07120-1/2023/269 from 10.5.2023.
[1] Forms were prepared by the IPRS and are available on this URL: https://www.ip-rs.si/obrazci/varstvo-osebnih-podatkov/ (15.7.2024).
[2] Transposition of Article 12(4) LED.
[3] Transposition of Article 12(4)(b) LED.
[4] Transposition of Article 13(1) and 13(2) LED.

1) *name and contact details of the competent authority: clear identification and contact points for the authority;*
2) *contact details of the data protection officer: information on how to reach the officer responsible for data protection;*
3) *purposes of data processing: detailed descriptions of why the personal data is being processed;*
4) *right to file a complaint with the supervisory authority: guidance on how individuals can lodge complaints and the necessary contact information;*
5) *right to access, correct, delete and restrict data processing, and to lodge complaints: explanation of the individual's rights regarding their personal data and how to exercise these rights, including the right to appeal to the supervisory authority;*
6) *legal basis for processing: the legal grounds justifying the data processing activities;*
7) *retention period or regular review dates for data retention: information on how long the data will be kept or when the need for its retention will be reviewed;*
8) *categories of data recipients, including international or third-party recipients: if available, details on who might receive the data, including recipients in third countries or international organisations;*
9) *additional information for exercising rights, especially if data was collected without the knowledge of the individuals: any other relevant details to help individuals exercise their rights, particularly if data was collected without their awareness.*

The information provided does not include the specific and technical details of how a data subject's personal data is processed in practice. However, the competent authority must publicly disclose information referred to in points 1 through 6,[5] while points 7 – 9 are disclosed to the individual upon request (see section 4.3 below). **From this perspective, the ZVOPOKD is broader than the LED, as the legal basis for personal data processing is considered general information and is accessible to individuals without a request.**

4.3 Right to access personal data

Before the implementation of the ZVOPOKD, individuals could access official police records containing their personal data based on the Personal Data Protection Act (ZVOP-1) (right to access their own personal data) or the ZNPPol (if they demonstrated a sufficient legal interest).[6] **The provisions of ZVOP-1 and ZNPPol now coexist with the ZVOPOKD, allowing individuals to choose which law to invoke when exercising their right to access personal data, depending on the specifics of their case.**

An individual has the right to request information from the competent authority about whether their personal data is being processed and to receive a copy or transcript of this data (Article 24(1) ZVOPOKD). Specifically, the individual[7] has the right to obtain detailed information about the following (Article 24(2) ZVOPOKD):[8]

[5] Examples can be found on the following sites:
Police: https://www.policija.si/o-slovenski-policiji/varstvo-osebnih-podatkov (12.7.2024).
Prosecutor's Office: https://www.dt-rs.si/varstvo-osebnih-podatkov (15.7.2024).
Courts: https://sodisce.si/informacije/varstvo_osebih_podatkov/#4-na-kaksni-pravni-podlagi-obdelujejo-sodisca-osebne-podatke-67 (15.7.2024).
[6] IPRS opinion 07121-1/2020/1408 from 12.8.2020.
[7] This right is not limited to individuals whose personal data is being processed. For example, parents requested the acquisition of personal data of their deceased son from the police. The IPRS pointed out to the parents Article 24 ZVOPOKD and 116 ZNPPol, according to which the police must provide data collected during the handling of an event or the performance of police tasks, upon a justified written request that must demonstrate circumstances from the fourth paragraph of Article 40 of the ZNPPol (demonstrated property and non-property damage, physical injury, suspicion of committing a criminal offence, and similar cases) to a person demonstrating a legal interest (IPRS Opinions 07121-1/2020/1618 from 16.9.2020 and 07121-1/2021/949 from 19.5.2021).
[8] Transposition of Article 14 LED.

a) *the purposes of processing and legal basis: the reasons and legal grounds for processing the data;*
b) *the types of personal data processed: categories of personal data being processed;*
c) *the recipients or categories of recipients: details of the recipients to whom the data has been disclosed, especially if they are in third countries or international organsations;*
d) *the retention period or review schedule: information on how long the data will be stored or when the need for its retention will be reviewed;*
e) *the rights to rectification, erasure, restriction and complaint: information on the individual's rights to correct, delete or restrict the processing of their data and to lodge complaints with the supervisory authority;*
f) *the right to lodge a complaint and contact information: details on how to file a complaint with the supervisory authority and its contact information;*
g) *the source of personal data: all available information about the origin of the personal data, unless the source's identity is protected as confidential.*

According to the IPRS, where two legal bases exist simultaneously, it is up to the individual to decide upon which the right to access personal data will be enforced. The IPRS provided an opinion to an individual who asked if it would be possible to obtain personal data of other individuals who were subjects of criminal proceedings in the same criminal case. The IPRS identified that under Article 24 ZVOPOKD, an individual can request access to personal data concerning them from the competent authority. According to Article 128 ZKP, anyone with a justified interest may be allowed to review and transcribe individual criminal records, while the accused has the right to review and transcribe records and view evidence. Therefore, the IPRS left it to the accused to decide which right to assert in their situation.[9]

When personal data could be used as evidence in a criminal investigation (this was the case of a video recording held by a third party, which could serve as exculpatory evidence), the IPRS took the position that if the competent authority had possession of the recording, the suspect could obtain it based on Article 24 ZVOPOKD. The evidence can also be obtained by an investigating judge and a state prosecutor since they are obliged, according to Article 17(1) ZKP, to truthfully and fully establish all facts relevant to issuing a lawful decision.[10] However, where a third party individual wants to obtain a video recording from the police, which is held as evidence in criminal proceedings, the IPRS stated that there must be a legal basis on the police's side for the transmission of the video recording (Article 116 ZNPPol) and a request in which the individual demonstrates a legitimate interest (Article 40 ZNPPol).[11]

Based on Article 25(1) ZVOPOKD, the individual's right to access their personal data may be partially or completely restricted, considering their human rights and fundamental freedoms, if such restrictions are necessary and proportionate for:[12]

a) *avoiding interference with or influence on official procedures to prevent, investigate, detect, or prosecute criminal offences or execute criminal sanctions;*
b) *avoiding interference with or influence on other related official procedures;*
c) *ensuring public safety;*[13]
d) *protecting the security or defence of the state;*
e) *protecting or exercising the human rights and fundamental freedoms of third parties.*

The competent authority must decide on any denial or restriction of access and provide the reasons for it without undue delay, within 15 days of receiving the request. This period can be

[9] IPRS Opinion 07121-1/2022/594 from 2.6.2022.
[10] IPRS Opinion 07121-1/2023/974 from 25.7.2023.
[11] Strangely, the IPRS did not point to Articles 24 and 25 ZVOPOKD (IPRS Opinion 07121-1/2023/754 from 5.6.2023).
[12] Transposition of Articles 13(3), 15(1) and 16(4) LED.
[13] In the LED, the term used is "public security" while Slovenian legislation refers to "public safety" without providing a definition, when it could encompass a broader set of issues or situations than "public security" does.

extended by up to 15 days if necessary, considering the complexity or number of requests. The decision must also include information on the right to appeal to the supervisory authority (Article 25(2) ZVOPOKD).[14]

In the denial decision, the competent authority does not include factual details or specific reasons if it would compromise the purpose of the denial.[15] Additionally, the decision must not confirm or deny the processing of personal data or restrictions on access (Article 25(3) ZVOPOKD). Instead, the specific reasons are included in a separate annex to the decision, which is not provided to the individual but is accessible to the data protection officer of the competent authority and the supervisory authority upon request, for performing oversight tasks related to the specific case (Article 25(5) ZVOPOKD).[16]

Article 25(3) ZVOPOKD is complemented by Articles 24(3) and 25(4), which regulate the particular case of covert investigative measures. **The competent authority must not provide information if doing so would hinder or affect official procedures, particularly if it would reveal the identity of individuals under covert investigative measures** as per the ZKP or ZNPPol (Article 24(3) ZVOPOKD). In such cases, the decision of the competent authority may not include (Article 25(4) ZVOPOKD):

1. *specific reasons for denial or restriction, if this would compromise the purpose of the denial or restriction;*
2. *confirmation or denial of personal data processing or of the restrictions on access to it.*

The competent authority must decide on the request without undue delay, and within one month of receiving the request. The decision must also include information on the right to appeal to the supervisory authority (Article 24(4) ZVOPOKD).

In another case involving the processing of location data from a mobile device by the police and a mobile operator for the purposes of a pre-trial procedure, the IPRS determined that the legal basis for processing such data lies in the provisions of the ZVOPOKD (Article 6(1)) in conjunction with ZKP (Article 149.b), which regulates the acquisition of metadata related to the communication of the suspect and/or victim for the purposes of investigating officially prosecutable criminal offences.[17] The IPRS also emphasised that although an individual has the right to access their personal data (Article 24 ZVOPOKD), this right can be restricted to prevent obstruction or influence on official proceedings related to law enforcement (Article 25 ZVOPOKD).[18]

The IPRS also dealt with a case where an individual believed the police were illegally reading their emails without a court order. The IPRS referred the individual to Article 24 of the ZVOPOKD, under which they could request access to their personal data from the police.[19] However, **the IPRS overlooked that access to email content constituted a covert investigative measure** (Article 150 ZKP), **and that the competent authority was not allowed to disclose such data to the individual** (Article 25(4) ZVOPOKD).

Notification to the individual targeted by covert investigative measures is regulated by the Criminal Procedural Act (ZKP). Notification happens only after the investigative judge's decision to formally start criminal prosecution or before the destruction of the data collected in case it is not used in subsequent prosecution proceedings. Article 154(2) provides two grounds for the investigative judge to restrict the right of information of the individual who was subjected to covert investigative measures: first, if it can be reasonably concluded that the disclosure "could threaten human life and health" and second, "due to other compelling reasons". **The latter seems to be an overly broad ground for restriction, which is unlikely to be in compliance with the necessity and proportionality requirements (in particular the clarity and foreseeability criteria) for any restriction of rights under EU law.**

[14] Transposition of Article 15(3) LED.
[15] Transposition of Article 15(3) LED.
[16] Transposition of Article 15(4) LED.
[17] IPRS Opinion 07121-1/2021/2638 from 5.1.2022.
[18] Ibid.
[19] IPRS Opinion 07121-1/2021/2621 from 3.1.2022.

In conclusion, the ZVOPOKD fully integrated the LED's right to access and its limitations in the Slovenian domestic legal order. It is worth noting, however, that the ZVOPOKD introduces an obligation on the competent authority – and not a possibility left at its discretion – to restrict the right to access when the disclosure would reveal a covert investigative measure.

4.4 Right to rectification or erasure of personal data and restriction of processing

Article 26 of the ZVOPOKD faithfully transposed Article 16 of the LED and its requirements in terms of the rights to rectification or erasure. There were neither individual cases that led the IPRS to adopt opinions specific to those matters nor relevant judicial proceedings. Therefore, we cannot draw conclusions at this stage on the implementation and effects of these provisions on data subject rights in Slovenia.

4.5 Remedies

4.5.1 Supervisory authority

The supervisory authority decides on the appeal of the individual whose personal data is processed against the decision of the competent authority (Article 27(1) ZVOPOKD).[20] There is no appeal against the decision of the supervisory authority, but administrative litigation is permissible (Article 27(2) ZVOPOKD).[21] In administrative litigation, the individual whose personal data is concerned, the competent authority, another controller or processor may file a lawsuit (Article 27(3) ZVOPOKD).

4.5.2 Proceedings in front of the courts

An individual who believes that a certain processing of their personal data by a competent authority or processor violates the provisions of the ZVOPOKD or other laws governing the processing or protection of personal data for law enforcement purposes, can request judicial review at any time as long as the violation persists, without prior exercise of rights under other provisions of the ZVOPOKD (e.g. appeal before the IPRS, i.e. the supervisory authority) or other legal remedies (Article 12(1) ZVOPOKD).[22]

With judicial protection, the individual can demand not only the cessation of the violation and the establishment of lawful conditions, but also compensation for damages (Article 12(2) ZVOPOKD).[23] If the violation has already ceased, the individual can file a lawsuit to establish that the violation occurred (Article 12(3) ZVOPOKD).[24]

However, in 2019 (before the enactment of Article 12(2) ZVOPOKD), an individual requested that the police delete their personal data, including photographs, fingerprints and a DNA profile. The police rejected the request, and the individual filed a lawsuit that the court dismissed. The individual's appeal was also rejected because they should have initiated an administrative procedure with the supervisory authority, which they did not do, thus not fulfilling the procedural precondition for a

[20] Transposition of Article 46(1)f LED.
[21] Transposition of Article 53(3) LED.
[22] Transposition of Article 54 LED.
[23] Transposition of Article 56 LED.
[24] The administrative court decides the proceedings according to the procedure defined by the Administrative Dispute Act (ZUS-1) for lawsuits concerning the violation of human rights and fundamental freedoms, and the individual can include a claim for damages in the lawsuit (Article 12(4) ZVOPOKD).

judicial process. The court[25] relied on the provisions of ZVOP-1 in force at the time, which stated that an individual has the right to request the supervisory authority's review of the competent authority's decision, and Articles 52 and 54 of the LED, which stipulate that every data subject has the right to lodge a complaint with the supervisory authority if they believe that the processing related to them infringes regulations adopted based on this directive. **Now that the ZVOPOKD applies, a similar lawsuit would be theoretically admissible if filed directly in front of the courts. The application of the LED in Slovenia therefore increased the number of avenues to access remedy for the individuals.**

5. Alignment of the legal basis for data processing with the LED

5.1 Data processing principles

Personal data may be processed for law enforcement purposes only to a limited extent and under specifically defined principles (Article 1(1) ZVOPOKD). The general guidelines for such processing by competent authorities are set out in Article 5 of ZVOPOKD, which transposes verbatim Article 4(1) of the LED into Slovenian law.

Based on the aforementioned article, competent authorities may process personal data only lawfully, fairly and transparently concerning the individual to whom the personal data relates. The processing of personal data is allowed only for specific, explicit and legitimate purposes, and it is not permitted to further process the data in a manner incompatible with these purposes (purpose limitation).

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation). Additionally, personal data must be accurate and, where necessary, kept up to date; competent authorities must take all reasonable steps to ensure that inaccurate personal data is erased or rectified without delay, considering the purposes for which it is being processed (accuracy and up-to-dateness).

The storage of personal data is permissible in a form that permits the identification of the individuals to whom the personal data relates, but only for as long as necessary for the purposes for which the personal data is processed (storage limitation). The processing operation must ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction, damage or loss of availability (integrity, confidentiality and availability).

5.2 Lawfulness of processing

The processing of personal data for law enforcement purposes is lawful only if it is necessary and to the extent required for the performance of tasks by competent authorities as determined by other laws (e.g. the Criminal Procedure Act - ZKP, which regulates police powers in criminal investigations).

The Higher Court in Celje, for example, dealt with a case in which a police officer accessed the personal data of 87 individuals without legal basis or reason. Although the personal data was

[25] Decision of the Administrative Court of the Republic of Slovenia I U 1971/2019-22 from 21.4.2021.

originally collected in a lawful manner, its processing by the police officer, which involved retrieving and consulting it, was declared unlawful because it was not part of any police or other official procedure involving these individuals. Police officers argued that the police also operates preventively by cooperating with the local community, hence their verification of certain personal data was legitimate, even in the absence of written documentation. The court emphasised that to ensure the legality of police powers, Article 130 ZNPPol stipulates that officers must report any use of police power in a work report or, if not writing a report, in a written act or an official note. These written acts must be produced no later than 24 hours after using the police power. The court stated: "This is also stipulated by Directive (EU) 2016/680 of 27 April 2016, which in Article 25 regulates the logging of processing operations and requires Member States to ensure logs are kept for at least the following processing operations in automated systems: collection, alteration, access, disclosure including transfers, combination, and erasure" (currently Article 47 of the ZVOPOKD). Therefore, **the court dismissed the officer's appeal because, in the absence of documentation, it was impossible to find the data processing lawful.**[1]

In one of its opinions, the IPRS emphasised that the processing of data is lawful only if the data is relevant and limited to what is necessary for the purposes for which it is processed (Article 5(3) ZVOPOKD). Processing is permissible to the extent necessary to perform the tasks of competent authorities (Article 6(1) ZVOPOKD), and by analogy, disclosure of personal data must be necessary for criminal proceedings.[2]

The types of personal data, categories of individuals to whom this personal data relates, the purpose of processing, and the storage period or the period for regular review of the necessity for storage must be defined by another law (Article 6(1) ZVOPOKD).[3, 4]

The specificity of the legal basis (*lex certa*) for personal data processing is of utmost importance according to the IPRS. In multiple cases, the data protection authority had to search and examine the legal basis for data processing by law enforcement and judicial authorities. It found that some of these processing operations lacked a sufficient legal basis:

- **Informing the police employing an individual who is subject to an investigation** about the conclusion and specific prosecutorial decisions by the Specialised State Prosecutor's Office - Department for Investigation and Prosecution of Officials with Special Powers: the IPRS pointed out Article 158.a ZKP as a legal basis, according to which the Special Department must inform the head of the authority where such an official is employed about the completed pre-trial procedure and the outcome of the procedure (either dismissal of the criminal complaint, request for investigation or filing of an indictment).[5]
- **Processing of the personal data of a convict during a prison sentence break**: the IPRS found the legal basis in Article 31 of the Enforcement of Criminal Sanctions Act (ZIKS-1).[6] This article further specifies that the data on convicts is collected directly from them, from other persons if the convict consents in writing, or from judicial authorities, the police, and other state bodies, public institutions, competent centres and local government bodies. And Article 38 of the ZIKS-1 stipulates that personal data from the database on convicts is

[1] Decision of the Higher Court in Celje PRp 179/2022 from 13.1.2023.
[2] IPRS Opinion 07121-1/2021/2663 from 18.1.2022.
[3] For example, the Residence Registration Act - ZPPreb-1, which in Article 42 regulates the guest register, specifying the types of personal data stored and the category of individuals (guests), authorises the police to manage and maintain the register, sets the data retention period (32 days), and defines the purpose of their storage, i.e. verifying guests' personal data in wanted persons records.
[4] Transposition of Article 8 LED.
[5] IPRS Opinion 07120-1/2021/244 from 12.5.2021.
[6] This article stipulates that the institution for the execution of prison sentences processes data on convicts serving prison sentences for the purpose of lawful and professional execution of criminal sanctions and informing victims about convicts serving prison sentences, about persons serving juvenile prison sentences, about minors subject to educational measures of placement in a correctional facility, and about persons subject to mandatory psychiatric treatment and protection in a health institution.

stored and used as long as the convict is serving a prison sentence. Therefore, the personal data of a convict, even if they are on a break from serving a prison sentence, can be processed.[7]

- **Records of stopped and inspected drivers and their travel direction**: the IPRS assessed that there is no legal basis for this processing as the ZNPPol does not regulate such records. Such data is recorded in the police officer's work report, which is only accessible to the unit leader or authorised persons. This is regulated with an internal document called the "Police Rules" that is not publicly available – which does not constitute a valid legal basis.[8] Consequently, in the absence of a proper legal basis, such data processing does not meet the principle of legality and is thus unlawful.
- **Identification of a person by a police officer without reason**: the IPRS concluded that establishing an individual's identity requires a specific reason according to Article 40 of the ZNPPol (e.g. the person needs to be detained, resembles a wanted person based on the description, enters a restricted area, arouses suspicion of committing a crime, etc.).[9]
- **Rejection by the police of a request made by a company owning a parking lot for personal data of the owner of a vehicle parked in a privately owned parking lot without a licence plate** based on the chassis number, although the company was incurring financial losses: the IPRS recalled that the police must have the appropriate legal basis for providing personal data about the vehicle owner. It referred to Article 64 of the Road Traffic Act (ZMV-1), which establishes a register of registered vehicles from which the police may obtain data, and Article 40 of the ZNPPol, which, among other things, stipulates that police officers may ascertain a person's identity at the request of a third party if the third party demonstrates pecuniary damage and an interest in asserting rights before the courts. Since the legal basis existed, the IPRS concluded that the company probably did not sufficiently demonstrate a legal interest (e.g. incurrence of financial loss).[10]
- **Police obtention of metadata from a mobile device that would indicate its use while driving**: the IPRS reviewed the multiple legal bases for obtaining metadata, specifically for accessing past metadata (Article 149.b ZKP), emergency calls (Article 134 Electronic Communications Act – ZEKom-1), internal procedures on responding to requests from competent authorities for access to users' personal data (Article 149 ZEKom-1), protection of life and physical integrity (Article 153.a ZEKom-1) and tracking malicious or nuisance calls (Article 155 ZEKom-1), and concluded that none of these legal bases fit the purpose of processing metadata from a mobile device in that particular case.[11]
- **Police inspection of the exterior of postal items (sender and recipient data) and related internal databases due to a criminal investigation**: the IPRS found that, given the existence of an appropriate legal basis (e.g. Article 115 ZNPPol) and provided it does not involve content protected by the confidentiality of communications, it is permissible for the police to inspect necessary postal databases (e.g. delivery records, records of undeliverable items, delivery books and inquiries) in connection with the inspection of postal items' exterior. The condition is that the inspection's purpose is limited to identifying items whose content would subsequently need to be inspected based on a court order.[12]

[7] IPRS Opinion 07120-1/2021/66 from 22 2.2021.
[8] IPRS Opinions 0712-3/2018/2307 from 30.12.2018 and 07121-1/2023/825 from 19.6.2023.
[9] IPRS Opinions 0712-1/2019/2328 from 14.10.2019, 07121-1/2021/2238 from 12.11.2021 and 07121-1/2023/1477 from 27.11.2023.
[10] IPRS Opinion 07121-1/2022/56 from 19.1.2022.
[11] IPRS Opinion 07121-1/2020/1573 from 10.9.2020.
[12] IPRS Opinions 07120-1/2020/489 from 28.8.2020 and 07120-1/2020/499 from 7.9.2020. However, it is essential to note that judicial practice and theory adopt a different stance, whereby postal service providers may disclose data about communication facts and circumstances only based on a court order due to the initiation or course of criminal proceedings (Križnar, P.: Commentary on Article 149.b, Criminal Procedure Act (ZKP) with commentary, Lexpera d.o.o., GV Založba, Ljubljana, 2023).

- **An individual requested an opinion on whether an electricity distributor could disclose the electricity consumption of a specific connection**: the IPRS took the stance that, in accordance with the then-applicable Energy Act (now the Electricity Supply Act (ZOEE)), the personal data processed includes personal name, address, tax number, metering point identifier, and metering and billing data. The legal bases for providing this data to the police are Article 148 ZKP, Article 112 and Article 115 ZNPPol. The IPRS concluded that the electricity distributor could disclose the electricity consumption of a specific connection to the police for the purpose of investigating a specific criminal offence.[13]

According to Article 6(2) ZVOPOKD, competent authorities may also process the personal data of an individual who has given consent[14] for the processing of their personal data for law enforcement purposes, if such a possibility, the purpose of processing, and the types of personal data to be processed are determined by another law.[15]

Moreover, competent authorities may exceptionally process personal data that is essential for protecting the life or physical integrity of the individual to whom the personal data relates or another person, considering the specific circumstances of the case (Article 6(3) ZVOPOKD).

If a competent authority has processed personal data for purposes other than those for which the data was collected, such further processing is permitted only if the data is processed for law enforcement purposes, and it is explicitly prescribed by law (Article 8(1) ZVOPOKD). Where personal data is processed for such other purposes, Regulation (EU) 2016/679 shall apply (Article 8(2) ZVOPOKD).[16]

In the context of the latter, the Higher Court in Ljubljana dealt with a suspect's complaint against a police officer's access to personal data records which would be contrary to their intended purpose. In this specific case, a police officer, while investigating an economic crime suspect, entered the suspect's personal data into the HOGO application – the national guest registration system – and obtained the information that the suspect stayed at a particular hotel. The suspect requested the exclusion of this evidence since the police officer accessed the record to investigate and detect the suspect's crime. They argued that the purpose is explicitly defined in Article 43 of the Residence Registration Act (ZPPreb-1), which is to maintain a guest register so that the police can cross-check guest data with the wanted persons' database (in which the suspect was not). The court agreed that the register's purpose differed from the one pursued by the access. However, it referred to Article 8(1) ZVOPOKD, which allows the processing of personal data by the same or another competent authority for purposes other than those for which the data were obtained if these purposes fall under those specified in Article 1(1) ZVOPOKD and are stipulated by law. Since investigating crimes and apprehending perpetrators is a fundamental police task specified by law (ZKP and ZNPPol) and aligns with the ZVOPOKD provisions, the court did not exclude the evidence.[17]

5.3 Sensitive personal data and the requirement of strict necessity

The definition of special categories of personal data is transposed verbatim into Slovenian legislation with **Article 4(12) ZVOPOKD**. They include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data,[18]

[13] IPRS Opinion 07121-1/2020/331 from 9.3.2020.
[14] This is based on the LED Recital n.35, which notably states: "This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive /.../".
[15] Consent for taking a buccal swab (Article 41(6) of the Police Tasks and Powers Act (ZNPPol)) or consent for polygraph testing under Article 48(2) of ZNPPol.
[16] Transposition of Article 9(1) LED.
[17] Decision of the Higher Court in Ljubljana V Kp 86510/2023 from 5.3.2024.
[18] Personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular,

biometric data[19] processed for the purpose of uniquely identifying an individual, data concerning health,[20] and data concerning an individual's sex life or sexual orientation.

The Slovenian legislator decided to prohibit in principle the processing of special categories of personal data (Article 7(1) ZVOPOKD). **This prohibition is not stricter than the legal framework of the LED, since the processing of special categories of personal data could still be performed by the competent authorities. Since the LED permits such processing only when strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only under specific conditions, similarly, the Slovenian legislator allowed the processing of special categories of personal data under certain conditions** (Article 7(2) ZVOPOKD).

These conditions are: (i) there must be a legitimate basis (legal foundation, individual's consent for processing, or necessity for protecting life or physical integrity); (ii) there must be statutory conditions and measures ensuring adequate protection of the human rights or fundamental freedoms of the individual whose special personal data is processed; and (iii) a) the processing of special personal data must be "absolutely necessary" for the performance of tasks by competent authorities, or b) the individual has explicitly made their special personal data public.

Since these cumulative conditions must be met for the processing of special categories of personal data, the legal basis in Slovenian law for processing sensitive personal data is more detailed and stricter than the legal basis for processing non-sensitive personal data. If these conditions are not met, processing is prohibited.

In practice, the IPRS consistently found that the cumulative conditions for processing sensitive data were met by competent authorities. The following cases illustrate this:

- **Submission of the medical documentation of a detainee to the ongoing criminal case file, and access to it** by persons authorised under Article 128 ZKP[21] to view the case file: the IPRS took the position that if a document is filed in the criminal case file according to the rules of criminal procedural law, from that moment onward, all persons entitled to access the case file under certain conditions specified by procedural legislation, within the so-called right to inspect the case file (Article 128 ZKP), are entitled to access the document. This also applies to medical documentation that has been obtained by the court or filed in the case file because the court deemed it necessary for deciding on detention conditions and other related issues.[22]
- **Disclosure of the patient's medical findings to the police for the performance of their duties** (investigating criminal offences, especially traffic accidents and bodily injuries) **without the patient's consent:** the IPRS took the position that the police can obtain health and other data about a patient from a healthcare provider without the patient's consent, but only for the purpose or needs of carrying out tasks from the police's statutory authority, e.g. investigating criminal offences.[23]
- **Access to the results of Covid-19 testing conducted by individuals, which were stored in written form or within a mobile application**: the IPRS took the position that, based on the legislation then in force, the police were authorised to conduct inspections of the implementation of restrictive measures to prevent the spread of infectious diseases.[24,25]

---

from an analysis of a biological sample from the natural person in question (Article 4(13) ZVOPOKD).

[19] 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) ZVOPOKD).

[20] Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status (Article 4(15) ZVOPOKD).

[21] Prosecutor, judge, defendant, attorney, private prosecutor, injured party as prosecutor, injured party, defence counsel, and any individual with a legitimate interest.

[22] IPRS Opinion 07121-1/2023/179 from 14.2.2023.

[23] IPRS Opinions 07121-1/2020/1453 from 24.8.2020, and 07121-1/2022/332 from 22.3.2022.

[24] Spreading infectious diseases is a criminal act according to Article 177. KZ-1.

[25] IPRS Opinion 07121-1/2021/674 from 7.4.2021.

- **Providing a physician's professional opinion on the patient's health condition to determine, in the pre-trial phase, whether the injuries are so severe as to meet the statutory elements of criminal offences**: the IPRS assessed that the ZKP (Article 148), ZNPPol (Articles 112 and 115) and State Prosecution Act (ZDT-1; Article 161) are satisfactory legal bases for processing this personal data, as these state bodies need them for the purpose of investigating and prosecuting criminal offences.[26]
- **Providing police with a medical report containing the patient's diagnosis** in order to ascertain, based on the diagnosed condition, whether the patient understood the significance of their actions on a specific day, define the patient's current health condition, and determine whether they could be interrogated: the IPRS took the position that when the police are investigating criminal offences (and thus there is an appropriate legal basis for performing police tasks – Article 148 ZKP, Articles 112 and 115 ZNPPol), the medical institution is obliged to provide the health report to the police in order to determine the suspect's capacity to participate in criminal proceedings. Additionally, the institution may (but is not obliged to) provide an opinion on the understanding of actions and the ability of the person to participate in the interrogation.[27]
- **Processing of biometric data, trade secrets or information covered by professional secrecy rules by the police**: the IPRS concluded that, based on Articles 33,[28] 112[29] and 115[30] of the ZNPPol, the legal basis is established if there is also an appropriate purpose for processing such data, such as investigating criminal offences.[31]

5.4 Prohibitions on certain types of processing

The ZVOPOKD explicitly prohibits the processing of personal data if such processing results in or involves unlawful discrimination based on nationality, race, skin colour, religion, ethnic origin, gender, language, political or other beliefs, sexual orientation, gender identity, property status, place of birth, education, social status, citizenship, place or type of residence, health status, genetic predispositions, or any other personal circumstances of an individual (Article 2 ZVOPOKD).

However, Article 2 ZVOPOKD does not in itself prohibit profiling, insofar as the ZVOPOKD or a sectoral law allows it and lays down the conditions and safeguards for it. Therefore, **the legislator has complemented Article 2 ZVOPOKD for automated profiling with Article 11(4) ZVOPOKD.** According to the latter, profiling based on automated or other processing of special categories of personal data that results in discrimination against individuals to whom the personal data relates is prohibited.[32]

In particular, automated profiling is prohibited if such decisions can negatively affect the legal status or rights of the individual or significantly impact them (Article 11(1) ZVOPOKD).[33] This is exceptionally permissible if a law provides that the individual whose data is being processed is entitled to: 1) request a review of the decision by a human being; 2) express their own viewpoint on

[26] IPRS Opinion 07120-1/2020/618 from 27.11.2020.
[27] IPRS Opinion 07120-1/2023/552 from 12.1.2024.
[28] The collection and processing of data is one of the police powers that police officers may exercise in carrying out police tasks.
[29] Police officers collect and process personal and other data, including data on the biometric characteristics of individuals and data from confidential relationships or professional secrets, when performing police tasks. Police officers collect personal and other data directly from the person to whom the data relates, and from others who have knowledge of such data, or from databases of personal data, official records, public books or other data collections.
[30] If police officers collect personal and other data about individuals from existing databases while performing police tasks, state authorities and legal persons who (based on the law and within the scope of their activities or in connection with them) maintain databases, must (upon a written or similar demonstrable request) provide the requested personal and other data free of charge.
[31] IPRS Opinions 07121-1/2024/19 from 11.1.2024 and 07121-1/2024/37 from 16.1.2024.
[32] Transposition of Article 11(3) LED.
[33] Transposition of Article 11(1) LED.

the decision; and 3) specify other measures to ensure adequate protection of human rights and fundamental freedoms by the competent authority.[34] However, even in this case, decisions cannot be based on the processing of special categories of personal data unless the law provides appropriate measures for the protection of human rights and fundamental freedoms and the legitimate interests of the individual concerned, such as the individual's consent to such processing (Article 11(2) ZVOPOKD).[35]

The provisions of the ZVOPOKD on unlawful discrimination, processing of special categories of data and automated profiling are therefore in line with the LED requirements.

6. New technologies and big data

6.1 Big data analytics

Slovenian national laws currently do not provide any specific legal basis for big data analytics[1] by the competent authorities. The closest approximation to such a legal basis would be Article 112(1) ZNPPol, which states that when police officers are investigating criminal offences, **they are allowed to process fingerprints and palm prints, photographs and DNA profiles in an automated manner** if this is necessary and essential based on the circumstances of the specific criminal offence.

In the opinion of this report's author, **this article, in conjunction with others, meets the criteria of Article 10 LED.** Processing special categories of personal data is permitted under this article only if it is absolutely necessary. Investigative actions are intended to secure evidence, thereby enabling the effective prevention, detection and prosecution of criminal offences, which also protects the human rights and fundamental freedoms of other individuals or other constitutional values (Article 15(3) Constitution). This is a constitutionally valid justification for interfering with the human rights and fundamental freedoms of both the accused and third parties through investigative actions.[2] Furthermore, adequate protection of the rights and freedoms of the individual, whose data is processed under Article 112 of the ZNPPol, is ensured. The individual is guaranteed the right to information (Article 23 of ZVOPOKD), the right to access personal data (Article 24 of ZVOPOKD and Article 127 of ZNPPol), and the right to rectify the data (Article 26 of ZVOPOKD). Concerning their data processing, they can file a complaint with the IPRS (Article 27 of ZVOPOKD) or initiate legal proceedings (Article 12 of ZVOPOKD). For data pertaining to an individual who is also a defendant and thus subject to criminal proceedings, the court is competent (Article 2 of ZKP), and the individual can also request the exclusion or review of the data's legality (Article 285.d of ZKP).

Additionally, one of the listed alternative conditions of Article 10 of the LED is fulfilled – **such processing is explicitly permitted by Article 112 of the ZNPPol.**[3] Moreover, the other two conditions under Article 10 LED (protection of the individual's vital interests or public disclosure of the data) could also be met, depending on the specific circumstances. **Consequently, Article 112 of the ZNPPol complies with the requirements of Article 10 of the LED.**

---

[34] Ibid.
[35] Transposition of Article 11(2) LED.
[1] Big data analytics could be considered a process of using machine learning, predictive modelling and statistical algorithms to analyse and examine large and complex data sets to uncover hidden patterns, correlations, trends and insights that can inform decision-making.
[2] Decision USRS U-I-115/14-28; Up-218/14-45 from 21.1.2016.
[3] In one of its decisions, the IPRS stated that, according to Article 112 ZNPPol, police officers are entitled to collect and process personal data to investigate criminal offences. Article 112 ZNPPol is also an appropriate legal basis, as required by Article 6 ZVOPOKD (IPRS Opinions 07121-1/2020/1495 from 31.8.2020, 07121-1/2022/1022 from 28.9.2022, and 07121-1/2023/1263 from 6.10.2023).

However, since automation in Article 112 of the ZNPPol is limited to specific personal data categories (biometric and genetic data) and there is no mention of predictive policing or artificial intelligence, it is the author's belief that this provision could not constitute a legal basis for big data analytics.

To support this conclusion, **Article 122(1) ZNPPol specifies that police may not solely use automated processing to produce a decision, proposal, criminal complaint or report** about a natural person, legal entity or other subject. If such automated processing could interfere with the rights or obligations of a natural person, legal entity or other subject, additional action and decisions must be taken by a police officer.[4]

Furthermore, through automated processing of personal or other data (especially by combining or comparing personal data from one or more databases of personal data, records, public registers or other collections of personal data) **the police are not, in principle, allowed to create personal profiles of individuals**. They may only do so if there is an **additional action and decision by a competent police officer in order to infer whether individuals have committed or have not committed a certain criminal act, or whether the statements of certain individuals are reliable or unreliable** (Article 122(2) ZNPPol).

Furthermore, automated processing of sensitive personal data for the purpose of creating a personal profile of a person is also prohibited (Article 122(2) ZNPPol).

Nevertheless, certain technologies in Slovenia could be considered big data analytics tools, some of which this report examines in the next section.

6.2 Technologies used in practice

6.2.1 Facial recognition

A German non-governmental organisation, Algorithm Watch, found that the Slovenian police has been using facial recognition technology since 2014.[5] This issue was first revealed in Slovenia by the NGO project Etičen.it,[6] which was subsequently covered by mainstream media.[7] Consequently, in 2021, **the IPRS initiated an inspection procedure against the police to assess the legality of personal data processing in the record of photographed persons**, which contains photographs of suspects of criminal offences taken by the police under Article 149(2) ZKP. The police provided several explanations, and during an inspection visit, the "Face Trace" system used for automated photo comparison was examined. **The IPRS inspection revealed "no systemic irregularities".**[8]

It was determined that the police uses facial photographs of individuals in the database of photographed persons for automated facial recognition purposes, by comparing them with the Face Trace module, which is an automated way of processing biometric data. **This is allowed under Article 112(1) ZNPPol solely for detecting and investigating criminal offences when necessary and essential given the circumstances of a specific crime,** which is in accordance with the LED as analysed in section 5.1 above**.**

[4] Like Article 11 ZVOPOKD.
[5] See: https://algorithmwatch.org/en/face-recognition-police-europe/ (15.7.2024).
[6] The Etičen.it project is run by Slovenian NGO Državljan D. (Citizen D), https://www.eticen.it/2019/12/12/slovenska-policija-in-biometrijske-metode-nadzora/ (15.7.2024).
[7] E.g. RTV SI, https://www.rtvslo.si/slovenija/tudi-slovenska-policija-uporablja-avtomatsko-prepoznavo-obrazov/510776; Dnevnik, https://www.dnevnik.si/1042917768; Oštro, https://www.ostro.si/si/razkrinkavanje/objave/policija-uporablja-orodje-za-prepoznavanje-obraza (15.7.2024).
[8] IPRS, 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 (15.7.2024).

The recognition process in the Face Trace module involves manually inputting a photo or footage (e.g. from a surveillance system) of a criminal suspect, which is then compared in an automated manner with photos of individuals stored in the photographed persons' database. The result is a list of individuals ranked by similarity to the suspect picture, and the final identification is always manually performed by a facial recognition expert.

The IPRS found no evidence that the Face Trace module could be used to automatically compare photographs online (or collected elsewhere, not yet stored in the police system) with those in the photographed persons' database. Thus, the system requires that the police first import the photo they wish to compare (e.g. publicly available on the internet or on open social media profiles) into their information system, where the comparison can then be made using the module. The police have established an adequate system to ensure an audit trail of personal data processing with the Face Trace module, allowing subsequent verification of the legality of data processing activities.

At the end of 2023, **the police announced that due to the obsolescence of the Face Trace module, they would transition to the field of forensic facial comparison facilitated by the Abis programme** (Automated Biometric Identification System).[9] This new programme will operate similarly to Face Trace, meaning it will only be used for investigating criminal offences and be based on photographs stored in the photographed persons' database. There is no further information available about this new system's functionalities or capacities, and it is therefore impossible to draw conclusions with regard to its compatibility with the law.

6.2.2 Drones

In 2017, the Slovenian Human Rights Ombudsman filed a request with the Constitutional Court of the Republic of Slovenia (*Ustavno sodišče Republike Slovenije* - USRS) to review the constitutionality and legality of Article 114.a(2)3 ZNPPol. This provision allows police officers to use unmanned aerial vehicles (drones) to "prove criminal offences and violations and to identify offenders among others".[10] **The Ombudsman argued that this provision was too general, introducing technology that enables continuous and pervasive surveillance, and that drones could be used in connection with any crime or violation handled by the police.** Consequently, the use of drones under such a provision would be disproportionate to the intended goal.

The Constitutional Court concluded that:

1) drones can be used to prove criminal offences and violations and to identify offenders;
2) they can only be used based on an already detected criminal offence or violation, which excludes their use for preventive or surveillance purposes in the sense of detecting illegal activities (e.g. traffic monitoring);
3) only technical means for photographing and recording audio and video are permissible on drones (excluding other technical means and weapons);
4) the use of drones is allowed only in the execution of police powers (Article 113 ZNPPol) where photographing and audio and video recording are already permitted, although previously these were used on other carriers and will now be permissible on unmanned aerial vehicles as carriers;
5) since Article 113 of the ZNPPol refers to other laws that establish a specific legal basis for the use of drones, they can only be employed when another law explicitly permits the use of these technical means.

[9] See: https://www.24ur.com/magazin/kako-bo-deloval-nov-policijski-sistem-za-prepoznavo-obrazov.html (15.7.2024).
[10] Other paragraphs under Article 114.a(2) ZNPPol allow the use of drones for other purposes such as to prevent and detect illegal crossings of the national border (Article 114.a(2)4). The USRS judgment solely focused on and interpreted the provision related to the use to "prove criminal offences and violations and to identify offenders among others".

As a result, the legal regulation of the use of drones was assessed by the USRS as constitutionally compliant.[11] The USRS based its assessment only on Slovenian primary law and did not consider referring the matter to the CJEU for a preliminary ruling on the compatibility of the Slovenian regulation of the use of drones with EU law.

Following the decision of the USRS, the police carried out a public procurement process, purchasing 24 unmanned aerial vehicles,[12] which are primarily used for border surveillance, searching for missing persons[13] and investigating criminal offences[14] in line with the other provisions of Article 114.a(2) ZNPPol.

The IPRS also addressed the use of unmanned aerial vehicles, specifically regarding their use within the framework of inspection supervision. The IPRS determined that, under Article 19(1) of the Inspection Procedure Act (ZIN), an inspector has the right to photograph or record visual data of persons, premises, objects, installations, etc. The ZIN does not specify which technical means an inspector can use for photographing and recording. However, the IPRS assessed that using unmanned aerial vehicles equipped with cameras and other sensors represents a significantly different approach to exercising inspection powers. This is because recording with an unmanned aerial vehicle generally captures a much larger area than recording with a camera or camcorder, which is usually directed at a specific object. According to the IPRS, the authorisation allowing an inspector to conduct photography and recording using an unmanned aerial vehicle in an inspection procedure should be explicitly stated in the law – which is not currently the case. Moreover, the inspector must also consider the principles related to the processing of personal data when obtaining such evidence.[15]

6.2.3 Licence plate recognition

The USRS assessed the constitutionality of Article 113(4) ZNPPol, which introduced a new technical means for automatic number plate recognition (ANPR) to carry out police tasks. The Slovenian Ombudsman argued that this legal provision conflicted with the right to privacy under Article 35 of the Constitution and the right to the protection of personal data under Article 38 of the Constitution. The challenged measure was considered disproportionate because, on one hand, it aimed only at combating vehicle theft, but on the other hand, it enabled the mass collection of location data for all traffic participants. The Ombudsman also deemed the further seven-day retention of data for the purpose of combating vehicle theft as disproportionate.

The USRS found that the measure of automatic licence plate recognition, as envisaged by the legislator, involves two different steps: the collection of data, and its subsequent comparison with other records of personal data. Both steps in data processing constitute separate interferences and require independently regulated legal frameworks for the processing of personal data. **Since the contested legislation did not stipulate that the collected licence plate data could be further processed through automatic (automated) comparison with other personal data records, the USRS concluded that the legislation was inconsistent with the legality requirement from the second paragraph of Article 38 of the Constitution.[16] Therefore, the USRS annulled it.[17] It is interesting to note once again that the USRS only carried out a constitutionality assessment and did not rely on EU law to reach its conclusion.**

---

[11] Partial decision USRS U-I-152/17-29 from 4.7.2019.
[12] See: https://www.rtvslo.si/slovenija/policija-kupuje-24-brezpilotnih-letalnikov-in-dva-kompleta-motilcev-signalov/464791 (15.7.2024).
[13] See: https://www.dnevnik.si/1042895951 (15.7.2024).
[14] See: https://www.policija.si/medijsko-sredisce/sporocila-za-javnost/sporocila-za-javnost-gpue/100443-uspesna-kriminalisticna-preiskava-celjskih-kriminalistov-zoper-tihotapce-ilegalnih-migrantov-le-eden-od-ukrepov-policije-za-ucinkovit-nadzor-drzavne-meje (15.7.2024).
[15] IPRS Opinion 07120-1/2023/538 from 20.12.2023.
[16] "The collection, processing, purpose of use, control, and protection of the confidentiality of personal data is determined by law."
[17] Partial decision USRS U-I-152/17-30 from 4.7.2019.

6.2.4 IMSI Catcher

The USRS assessed the conformity of Article 150.a ZKP with the Constitution. This provision regulates the uses and purposes of special technical means for monitoring mobile telephony signals, known as IMSI catchers.[18] The ZKP regulates the conditions for their use, the content of the report on their use, and the handling of personal data of third parties. It also introduces a prohibition on using IMSI catchers for intercepting communication content for persons who are not suspects or defendants, and regulates the exclusion of evidence. With an IMSI catcher, the police obtain the data necessary to identify the number of the communication device and electronic communication numbers, as well as data on the location of the communication device.[19]

The USRS found that the ZKP does not contain provisions enabling comprehensive subsequent judicial control over the use of IMSI catchers. In other words, there are no measures in the law that ensure that the investigating judge has a precise overview of the use of IMSI catchers, and the data obtained thereby.

Additionally, the law does not contain provisions ensuring actual control over the location of the IMSI catcher when it is not in use. Consequently, **the investigating judge is deprived of effective subsequent judicial review of the use of IMSI catchers and their oversight**, thus impeding effective subsequent judicial review of constitutional and legal conditions for interfering with the right to privacy under Article 37 of the Slovenian Constitution.

Therefore, the USRS decided that the use of IMSI catchers based on the legal framework is inconsistent with the right to informational privacy under Article 38 of the Constitution, and annulled the legislation.[20]

6.2.5 AlgoLex

In 2021, **a proof-of-concept for automated legal decision-making within criminal proceedings was established in Slovenia for the first time.**[21] This system uses supervised machine learning algorithms and publicly available historical data from court decisions.[22] It aims to assist judges,

[18] The IMSI catcher mimics a legitimate cell tower, tricking nearby mobile phones into connecting to it instead of the real network tower. Once a mobile phone connects, the IMSI catcher captures the phone's unique IMSI number and other metadata, which allows law enforcement or other operators to identify and track the user. By triangulating the phone's location based on signal strength or by connecting to multiple IMSI catchers, the device can be also used to approximate the user's position.

[19] The IMSI catcher works by simulating the operator's base station. It (falsely) presents itself to electronic devices within its range as the strongest base station of one of the operators. The electronic device therefore provides the IMSI catcher with its IMEI and the IMSI of the inserted SIM card as part of the authentication process. The IMSI catcher can also be used to determine the location of the electronic device. The IMSI catcher can ask the electronic device to amplify its signal, and by moving the IMSI catcher it can be determined whether the signal strength is decreasing or increasing. The higher the signal strength, the closer the IMSI catcher is to the electronic device and *vice versa* (Križnar, P.: Commentary on Article 150.a, Criminal Procedure Act (ZKP) with commentary, Lexpera d.o.o., GV Založba, Ljubljana, 2023).

[20] Partial decision USRS U-I-144/19-46 from 1.12.2022.

[21] URL: www.algolex.si (15.7.2024). See also: Križnar, P. and Piršič, K.: "Detention Decision-Making in Slovenia Using the Computerized Risk Assessment Tool Detention v1.0: Effective Use of Machine Learning Algorithms from the Perspective of the Defendant's Procedural Rights." In: Završnik, A., Badalič, V. (eds) *Automating Crime Prevention, Surveillance, and Military Operations*, Springer 2021, and Križnar, P. Piršič, K. and Marinšek, T.: "Using machine learning to assess risk of recidivism in detention decisions." In: Završnik, A. (ed) *Law and artificial intelligence: issues of ethics, human rights and social harm*, Institute of criminology at the Faculty of Law in Ljubljana 2021.

[22] The level of the prescribed sentence for the offence, the role of the defendant in the offence, the stage of the offence, the number of offences, the organisation of the offence, the use of dangerous means, the elements of violence (details of the criminal offence), gender, age, level of education, employment, financial situation, marital status, dependent children or family members, whether the defendant is the subject of

prosecutors and attorneys in determining the criminal sanction for the offence of unlawful production and trafficking of narcotic drugs under Article 186(1) of the Criminal Code (KZ-1), as well as assessing the risk of recidivism when deciding on detention.[23]

Even if it remains unclear whether some or all phases of a criminal trial fall within the scope of the LED,[24] certain provisions of the ZVOPOKD apply *mutatis mutandis* to criminal matters. Thus, when a criminal matter means the exercise of judicial power, which includes the carrying out of investigations and inquiries, the trial and the hearing of appeals in a criminal matter fall within the jurisdiction of the courts of general jurisdiction as defined by the law governing the courts.

It is important to note that the AlgoLex algorithm is not currently in use and serves as a demonstration for the public. Furthermore, it is considered to be not solely based on automated processing, as it theoretically involves meaningful human involvement in the decision-making process. The judge would be the main legal subject during the criminal proceedings. They would still lead the hearing, gather general information about the defendant, verify it, inform the defendant of the criminal offence, and explain to them the grounds for the charges against them. The judge would also instruct the defendant of their right not to self-incriminate, question them, rule upon the motion of the state prosecutor, and manually review the automated result upon the individual's request to do so. Besides the judge, there would still be other humans involved in the process: a mandatory attorney next to the defendant and the state prosecutor.[25] Human judgment would also be required to verify the machine-generated decisions, ensuring that they are not solely reliant on automation. **Given that this was an experimental project and not used in real conditions, it remains uncertain whether this human involvement could actually be meaningful.**

Since the solution is not supposed to replace the judge's decision but only to provide technical support by assessing the particular circumstances of the case and analysing past decisions, it likely falls outside the scope of the general prohibition on automated decision-making outlined in Article 11(1) of the ZVOPOKD.

7. Conclusion

Although Slovenia missed the deadline for transposing the LED into its legal framework, it was eventually transposed through the ZVOPOKD. **Many provisions of this law are either directly copied or closely aligned with the wording of the LED.** There are no issues regarding the scope of the LED, as the ZVOPOKD clearly defines both the concept of a competent authority (personal scope) and the notion of a criminal offence (material scope). The enforcement of the LED is

parallel criminal proceedings, the number of previous criminal convictions, any breaches of probation, the number of previous misdemeanour convictions (details of the defendant), the defendant's dependence on alcohol or drugs, the defendant's residency, whether the defendant makes their living by committing criminal offences and the existence of behavioural or other personal characteristics of the defendant (information provided by the court).

[23] The circumstances are: the severity of the prescribed penalty for the criminal offence, the defendant's role in the crime, the stage of the criminal act, the number of criminal offences, the level of organisation of the crime, the use of dangerous instruments (such as guns, knifes, screwdrivers, etc.), elements of violence, gender, age, education level, employment status, financial situation, relationship status, dependent children or family members, whether there are parallel criminal proceedings against the defendant, the number of prior convictions for criminal offences, the type of repeat offender, any violations of probation, the number of prior convictions for misdemeanours related to the crime, the defendant's dependency on alcohol or illegal drugs, the condition of their residence, whether the defendant sustains themselves through criminal activities, and the presence of deviant behavioural or personality traits.

[24] Vogiatzoglou P. and Marquenie T.: Assessment of the implementation of the Law Enforcement Directive, EPRS, PE 740.209 - December 2022, URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf

[25] See Križnar, P. and Piršič, K., 2021.

entrusted to the IPRS, which also oversees the enforcement of the General Data Protection Regulation (GDPR).

Time limits for the erasure of personal data or periodic reviews of the necessity to retain such data are regulated by sectoral laws, such as Article 128 of the Police Tasks and Powers Act (ZNPPol), rather than the ZVOPOKD. Therefore, the general requirement under Article 5 of the LED is fulfilled.

The legal basis for data processing, as required by Article 8 of the LED, is also outlined in sectoral legislation. Given the same requirement in Article 38(2) of the Slovenian Constitution, an exact legal basis is crucial when supervisory authorities or courts assess the legality of data processing. This is particularly important for processing special categories of personal data, which is generally prohibited, but exceptions under the LED allow processing under strict cumulative conditions, outlined in Article 7(2) of the ZVOPOKD. Because these conditions must be met for the processing of special categories of personal data, the legal framework for processing sensitive personal data in Slovenia is more detailed and stricter than for non-sensitive data. If these conditions are not met, processing is prohibited.

Regarding automated decision-making, Slovenian law is aligned with the LED, requiring that such decisions are not based on special categories of personal data unless appropriate safeguards are in place. Profiling that leads to discrimination is also prohibited. Moreover, national legislation provides for appropriate safeguards to protect the rights and freedoms of data subjects in cases where automated decision-making is permitted by law.

Slovenia has opted to use the LED's provision to restrict data subjects' right of access to their personal data. The competent authority is not required to provide information if doing so would obstruct or compromise official procedures, particularly if it would reveal the identities of individuals under covert investigative measures. Furthermore, individuals' rights to access their personal data may be partially or entirely restricted if such limitations are necessary and proportionate for the prevention or detection of crime, public safety, state security or defence, or the protection of third parties' human rights and fundamental freedoms. These exemptions are clearly outlined in the ZVOPOKD, and data controllers have no discretion in their application.

Considering the scope of this report, the relevant national provisions are in compliance with the LED, and no legal gaps have been identified. Consequently, no further legislative action is required. However, it should be noted that these provisions are not frequently applied in practice by competent authorities, making it difficult to assess the practical implementation of the LED. **Since the adoption of the ZVOPOKD, the IPRS has mainly issued non-binding legal opinions, and only a few court rulings are available – none of which interpret the ZVOPOKD directly, but only indirectly. Notably, the Slovenian Constitutional Court (USRS) had to assess a number of cases involving the use of technologies and "modern" data processing techniques for law enforcement purposes but did not rely on EU law, and in particular the LED, to evaluate the conformity of the Slovenian legislation.**

Careful consideration will be necessary when the legislature is drafting or amending laws related to big data analytics. Furthermore, some technological solutions (GPS tracking, automated judicial decision-making, and facial recognition) lack a clear legal basis, while others (IMSI catchers and licence plate recognition systems) have insufficient legal foundations. Otherwise, no specific recommendations are necessary.

8. Literature

8.1 Laws

Criminal Code (**KZ-1**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 50/12, 54/15, 6/16, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 and 16/23.

Criminal Procedure Act (**ZKP**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 176/21, 96/22, 2/23 and 89/23.

Electricity Supply Act (**ZOEE**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 172/21.

Electronic Communications Act (**ZEKom-1**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 109/12, 110/13, 40/14, 54/14, 81/15, 40/17, 189/21 and 130/22.

Employment Relationships Act (**ZDR-1**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 21/13, 78/13, 47/15, 33/16, 52/16, 15/17, 22/19, 81/19, 203/20, 119/21, 202/21, 15/22, 54/22, 114/23 and 136/23.

Enforcement of Criminal Sanctions Act (**ZIKS-1**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 110/06, 76/08, 40/09, 9/11, 96/12, 109/12, 54/15, 11/18, 200/20 and 141/22.

General Administrative Procedure Act (**ZUP**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 24/06, 105/06, 126/07, 65/08, 8/10, 82/13, 175/20 and 3/22.

Inspection Procedure Act (**ZIN**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 43/07 and 40/14.

Personal Data Protection Act (**ZVOP-1**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 94/07, 177/20 and 163/22.

Personal Data Protection Act (**ZVOP-2**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 163/22.

Personal Data Protection Act in the Field of Criminal Offences (**ZVOPOKD**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 177/20.

Police Tasks and Powers Act (**ZNPPol**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 15/13, 23/15, 10/17, 46/19, 47/19 and 153/21.

Residence Registration Act (**ZPPreb-1**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 52/16, 36/21 and 3/22.

Road Traffic Act (**ZMV-1**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 75/17 and 92/20.

State Prosecution Act (**ZDT-1**), Official Gazette of the Republic of Slovenia [Uradni list RS], no. 58/11, 21/12, 47/12, 15/13, 47/13, 48/13, 19/15, 23/17, 36/19, 139/20, 54/21 and 105/22.

8.2 Decisions of the courts

Decision of the Administrative Court of the Republic of Slovenia I U 1971/2019-22 from 21 4.2021

Decision of the Constitutional court of the Republic of Slovenia U-I-152/17-30 from 4.7.2019

Decision of the Constitutional court of the Republic of Slovenia U-I-144/19-51 from 6.7.2023

Decision of the Constitutional court of the Republic of Slovenia U-I-115/14-28; Up-218/14-45 from 21.1.2016

Decision of the Court of Justice of the European Union C-817/19 from 21.6.2022

Decision of the Higher Court in Celje PRp 179/2022 from 13.1.2023

Decision of the Higher Court in Ljubljana V Kp 86510/2023 from 5.3.2024

Partial decision of the Constitutional court of the Republic of Slovenia U-I-152/17-29 from 4.7.2019

Partial decision of the Constitutional court of the Republic of Slovenia U-I-152/17-30 from 4.7.2019

Partial decision of the Constitutional court of the Republic of Slovenia U-I-152/17-69 from 17.11.2022

Partial decision of the Constitutional court of the Republic of Slovenia U-I-144/19-46 from 1.12.2022

8.3 Scientific articles

Križnar, P.: Commentary on Article 149.b, 150.a, Criminal Procedure Act (ZKP) with commentary, Lexpera d.o.o., GV Založba, Ljubljana, 2023.

Križnar, P. and Piršič, K.: "Detention Decision-Making in Slovenia Using the Computerized Risk Assessment Tool Detention v1.0: Effective Use of Machine Learning Algorithms from the Perspective of the Defendant's Procedural Rights." In: Završnik, A., Badalič, V. (eds) *Automating Crime Prevention, Surveillance, and Military Operations*, Springer 2021.

Križnar, P. Piršič, K. and Marinšek, T.: "Using machine learning to assess risk of recidivism in detention decisions." In: Završnik, A. (ed) *Law and artificial intelligence: issues of ethics, human rights and social harm*, Institute of criminology at the Faculty of Law in Ljubljana 2021.

8.4 Opinions of the IPRS

0712-3/2018/2307 from 30.12.2018

0712-1/2019/2328 from 14.10.2019

07121-1/2020/331 from 9.3.2020

07121-1/2020/1408 from 12.8.2020

07121-1/2020/1453 from 24.8.2020

07120-1/2020/489 from 28.8.2020

07121-1/2020/1495 from 31.8.2020

07120-1/2020/499 from 7.9.2020

07121-1/2020/1573 from 10.9.2020

07121-1/2020/1618 from 16.9.2020

07120-1/2020/618 from 27.11.2020

07120-1/2021/66 from 22.2.2021

07121-1/2021/674 from 7.4.2021

07120-1/2021/244 from 12.5.2021

07121-1/2021/949 from 19.5.2021,

07121-1/2021/2238 from 12.11.2021

07121-1/2021/2621 from 3.1.2022

07121-1/2021/2638 from 5.1.2022

07121-1/2021/2663 from 18.1.2022

07121-1/2022/56 from 19.1.2022

07121-1/2022/125 from 3.2.2022

07121-1/2022/332 from 22.3.2022

07121-1/2022/594 from 2.6.2022

07121-1/2022/1022 from 28.9.2022

07121-1/2023/179 from 14.2.2023

07121-1/2023/203 from 17.2.2023

07121-1/2023/391 from 5.4.2023

07120-1/2023/269 from 10.5.2023

07121-1/2023/754 from 5.6.2023

07121-1/2023/825 from 19.6.2023

07121-1/2023/974 from 25.7.2023

07121-1/2023/1263 from 6.10.2023

07121-1/2023/1477 from 27.11.2023

07121-1/2023/1223 from 3.1.2024

07121-1/2024/19 from 11.1.2024

07120-1/2023/552 from 12.1.2024

07121-1/2024/37 from 16.1.2024

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights