Personal Data Protection:
Views, Opinions and Practice of the Commissioner

Publication No. 11

Publisher
Commissioner for Information of Public Importance
and Personal Data Protection
15 Bulevar Kralja Aleksandra, 11000 Belgrade
Tel: +381 11 3408 900
Fax: +381 11 3343 379
E-mail: office@poverenik.rs
www.poverenik.rs

For the Publisher
Milan Marinović

Editor
Sanja Unković

Proofreading, design and layout
Official Gazette

Printing
Official Gazette

Print run
500 copies

ISBN 978-86-82712-07-7

Belgrade, 2026.

Commissioner for Information
of Public Importance and
Personal Data Protection

Personal Data Protection: Views, Opinions and Practice of the Commissioner

Content

FOREWORD

Dear reader,

You who are holding in your hands the most recent of eleven publications that the Commissioner has steadfastly issued each year to mark International Data Protection Day — and you who are, at this very moment, reading the foreword I wrote some time ago, though not in the distant past — can see for yourself that my earlier prediction, or more precisely my concern, expressed in the tenth publication that this edition might appear solely in digital form, or in an even more modern format, has not materialised.

In my humble opinion, this is fortunate! Although you will need to find a little extra space on your bookshelf — just enough to accommodate the thickness of this volume — so that it may take its rightful place beside its ten predecessors. And like them, it is not meant to gather dust, but to be taken up and read whenever you wish to learn how, in 2025, the Commissioner dealt with cases of employers monitoring employees through GPS-based technology; or how the Commissioner responded when a Controller sent an email to all recipients in a way that allowed each of them to see the personal data of others contained in the message. Or how the Commissioner intervened in a case where, during the delivery of documents via a notice board, certain technical, organisational and staffing measures had not been undertaken, resulting in a breach of the Law on Personal Data Protection; and in another case involving the unlawful processing of medical records and health data. As in previous editions, this publication also includes several examples concerning the use of video surveillance in the processing of personal data.

The section dedicated to the Commissioner's practice in safeguarding data subjects' rights this year also features examples in which the Commissioner found that the conditions for exercising the right to erasure had not been met. It also contains a series of answers provided by the Sector for Harmonisation of Regulations and Normative Affairs within the Commissioner's Office to various questions relating to the exercise of personal data protection rights.

I would also like to take this opportunity to acquaint you with an activity of exceptional importance for the future realisation of this right. At the time of writing this foreword, work on the new Law on Personal Data Protection is well advanced, making it reasonable to expect that the next publication will be issued during the implementation of a new, clearer, more

precise, more modern and therefore more effective law, fully aligned with the needs of the contemporary age.

And what is the future of publications such as this one in the years ahead?

That future is secure, and indeed bright. This is because the development of society — not only in Serbia but across the world — is moving inexorably towards increasing digitalisation and the ubiquitous use of modern technologies, not to mention artificial intelligence. This inevitably brings heightened risks to some fundamental human rights, particularly those within the sphere of privacy, such as the right to personal data protection.

Consequently, it is to be expected that the Commissioner, as the primary authority for the protection of this right in Serbia, will be required to devote ever more attention and effort to its safeguarding — which, quite naturally, will lead to new publications in the years to come.

With the hope that, with the Commissioner's continued key role, this important and increasingly vulnerable right will be preserved to the extent necessary.

Editor
Sanja Unković

1. ESTABLISHING THE FACTUAL SITUATION IN SUPERVISORY PROCEEDINGS

The Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) conducts supervision and ensures the application of the Law on Personal Data Protection (Official Gazette of the Republic of Serbia, No. 87/2018; the Law has been in force since 22 August 2019)[1] *(hereinafter: the LPDP), in accordance with the Commissioner's competences.*

Under Article 79 of the LPDP, the Commissioner is empowered to take the following corrective measures: to warn the Controller and the Processor, by issuing a written opinion, that the envisaged processing operations may infringe the provisions of this Law, in accordance with Article 55, paragraph 4 of this Law; to issue a warning to the Controller or Processor where the processing infringes the provisions of this Law; to order the Controller and Processor to act upon the request of the data subject for the exercise of his or her rights under this Law; to order the Controller and Processor to bring the processing operations into compliance with the provisions of this Law in a precisely defined manner and within a precisely defined deadline; to order the Controller to notify the data subject of a personal data breach; to impose a temporary or permanent restriction on processing, including a prohibition of processing; to order the rectification or erasure of personal data, or the restriction of processing, in accordance with Articles 29 to 32 of this Law, and to order the Controller to notify another Controller, the data subject and the recipients to whom personal data have been disclosed thereof, in accordance with Article 30, paragraph 3 and Articles 33 and 34 of this Law; to revoke a certificate or to order the certification body to revoke a certificate issued in accordance with Articles 61 and 62 of this Law, as well as to order the certification body to refuse to issue a certificate if the conditions for its issuance have not been met; to impose a monetary fine by means of a misdemeanour order where, during an inspection, it is established that a misdemeanour has been committed for which this Law prescribes a fixed monetary fine, instead of or in addition to other measures prescribed under this paragraph, depending on the circumstances of the specific case; and to suspend the transfer of personal data to a recipient in another state or an international organisation.

If, during an inspection, the Commissioner determines that the LPDP has been infringed, the Commissioner submits a request for the initiation of misdemeanour proceedings, and for misdemeanours for which a fixed monetary fine is prescribed, issues a monetary fine by means of a misdemeanour order.

---

1 LPDP („Official Gazette of RS", number 87/2018)
The application of the Law commenced on 22 August 2019.

1.1. The Controller processed employees' data during the use of official vehicles through the application of global positioning system (GPS) technology.

From the operative part:

The Commissioner issued a Warning to the Controller because the Controller had processed the personal data of employees who had used the Controller's official vehicles equipped with a satellite vehicle-tracking system (GPS), without an appropriate legal basis under Article 12, paragraph 1 of the LPDP, thereby infringing the principles of "lawfulness, fairness and transparency", "storage limitation" and "accountability" set out in Article 5, paragraph 1, points 1) and 5), and paragraph 2 of the same Article of the LPDP, respectively.

From the reasoning:

The Controller claimed that the purpose of processing personal data through the use of GPS was the protection of the Controller's property, namely determining the location of a vehicle in the event of theft and/or unauthorised use, monitoring the vehicle's speed (due to employees' misdemeanour liability) in order to detect risky driving behaviour in relation to traffic regulations and safety, and enabling timely intervention to provide assistance to an employee in cases of traffic accidents or vehicle breakdowns. The Controller further claimed that the processing of employees' personal data using GPS was based on legitimate interest; however, the Controller did not submit to the Commissioner any document that would justify reliance on legitimate interest as the legal basis for the described processing, and that would contain a prior assessment of the relevant aspects of the envisaged processing, allowing the Commissioner to evaluate whether the conditions prescribed by Article 12, paragraph 1, point 6) of the LPDP had been met.

The protection afforded by the LPDP would be unacceptably weakened if the use of GPS were permitted at any cost and without a careful balancing of the possible benefits of using GPS against the important interests of safeguarding private life. GPS enables the real-time tracking of a vehicle's movement, making it possible to identify the geographic location of the person or persons presumed to be using the vehicle at any given moment or on an ongoing basis. Although the processing of personal data for the purpose of protecting the Controller's property may, in principle, be justified by legitimate interest as a lawful basis for processing, the Controller in this case failed to demonstrate that the manner of processing was appropriate and necessary for achieving the stated purpose, nor did the Controller present any evidence of past incidents involving (attempted) vehicle theft, unauthorised vehicle use, or any justified risk that such incidents might occur.

With regard to the protection of property and individuals, the Commissioner takes the view that the continuous use of GPS is excessive, since the locations where a traffic accident and/or vehicle breakdown occurs can be (and in the vast majority of cases are) reported by the driver, and that less intrusive methods are available to the Controller for achieving that purpose. As for potentially risky driving behaviour in relation to traffic regulations, the Controller is advised that monitoring compliance with road traffic safety regulations falls within the competence of the traffic police, and that the processing of personal data by means of GPS for that purpose is disproportionate, particularly given that the Controller did not present to the Commissioner any evidence that employees, when using official vehicles, exceeded permitted speed limits or behaved in a risky manner in traffic.

By processing personal data for the purposes stated in the Controller's written submission, relying on legitimate interest, the Controller is processing employees' personal data without an appropriate legal basis under Article 12, paragraph 1, point 1) of the LPDP, and in a manner that infringes the principle of "lawfulness, fairness and transparency" set out in Article 5, paragraph 1, point 1) of the LPDP, since the data are not processed lawfully, fairly or transparently in relation to the data subjects. The Controller also failed to provide the Commissioner with any document that would justify the reliance on legitimate interest as the legal basis for the described processing, and that would include a prior assessment of the relevant aspects of the intended processing; therefore, the Controller did not succeed in defending legitimate interest as the lawful basis for the processing concerned. Furthermore, the non-transparent nature of the Controller's storage of data collected through GPS indicates that the storage period is not limited, i.e. that the data are stored permanently, thereby infringing the principle of "storage limitation" under Article 5, paragraph 1, point 5) of the LPDP. The permanent storage of data, as occurs in this case, creates an unfair imbalance between opposing public and private interests and thus constitutes a disproportionate interference with the rights of the data subjects and cannot be considered necessary in a democratic society. Through the described manner of processing personal data using GPS, the Controller also failed to demonstrate compliance with the principles laid down in Article 5, paragraph 1 of the LPDP, thereby infringing the principle of "accountability" under Article 5, paragraph 2 of the LPDP.

In view of all the foregoing, the Controller is advised that, in the present case, among the six conditions prescribed by Article 12, paragraph 1 of the LPDP, the only possible basis for processing the personal data of natural persons is consent — consent which must be freely given, unconditional, specific, granular, informed, unambiguous, documented, and which must be capable of being withdrawn at any time.

Action taken by the Controller:

The Controller submitted to the Commissioner a notification stating that it had ceased using GPS, namely that the period for which the GPS service had been contracted with the Processor had expired, that the service had not been extended or subsequently contracted again, and that the devices installed in the vehicles for tracking purposes had been removed. The Controller also submitted, as evidence, an appropriate confirmation of the removal of the devices issued by the Processor, following which the Commissioner concluded the proceedings in this case.

Case Number: 072-04-2384/2024-07

1.2. The Controller sent several documents to a large number of e-mail addresses in such a way that all recipients' e-mail addresses were visible to every individual recipient of the e-mail

From the operative part:

The Commissioner issued a Warning to the Controller because the Controller failed to take appropriate personal data protection and security measures, in accordance with Article 42, paragraph 1, point 2) of the LPDP and Article 50, paragraphs 1–3 of the LPDP, and consequently, by sending the e-mail, unlawfully disclosed the personal data of a large number of individuals, thereby acting contrary to the principle of "integrity and confidentiality" set out in Article 5, paragraph 1, point 6 of the LPDP.

From the reasoning:

As it was established that the Controller sent an e-mail to recipients in such a manner that all recipients' e-mail addresses were visible to every individual recipient, thereby resulting in the unauthorised disclosure of and access to the personal data contained in those e-mail addresses, the Controller acted contrary to the provisions of Article 42 of the LPDP cited in the operative part. Specifically, the Controller failed to implement appropriate technical, organisational and staffing measures and failed to ensure the application of necessary safeguards during processing, in order to meet the conditions for personal data processing prescribed by the LPDP and to protect the rights and freedoms of the data subjects. The Controller also acted contrary to Article 50 of the LPDP, concerning the security of processing, thereby infringing the principle of "integrity and confidentiality" set out in Article 5, paragraph 1, point 6 of the LPDP.

When issuing this Warning, the Commissioner took into account the fact that no data subject whose personal data had been compromised in the

manner described had contacted the Commissioner in this case, as well as the fact that the Controller had at its disposal measures enabling the protection of the anonymity of e-mail recipients for the purpose for which the data had been collected, but failed to use them.

Action taken by the Controller:

Acting upon the Warning, the Controller informed the Commissioner that, in order to remedy the breach of the LPDP, it had deleted the mailing list containing all the relevant e-mail addresses, had decided not to use them in any manner in the future, and would henceforth apply all necessary protection mechanisms and measures to prevent further breaches of the LPDP.

Case Number: 072-21-2336/2025-07

1.3. Processing of primary school pupils' parents' personal data in the course of electronic communication via e-mail

From the operative part:

The Commissioner issued a Warning to Primary School X, as the personal data controller, because, in the course of electronic communication with pupils' parents via e-mail, it processed personal data in a manner that made all recipients' e-mail addresses visible to each individual recipient, thereby infringing Article 5, paragraph 1, point 3 of the LPDP, as the processing in question was not carried out in a manner that ensures data minimisation, and Article 52, paragraph 1 of the LPDP, as the School failed to notify the Commissioner of the personal data breach that occurred during the processing concerned.

From the reasoning:

In the course of the inspection supervision procedure, it was established, inter alia, that: on the day in question, two e-mails were sent from the e-mail address of the School's Assistant Principal to more than 100 parents of pupils — one concerning information on the delivery of teaching and the other concerning an announcement regarding the work of the School's governing bodies; that the e-mails in question were sent in such a way that all recipients' e-mail addresses were entered into the "To" field, instead of the "Bcc" (Blind Carbon Copy) field, thereby disclosing the e-mail addresses of all recipients to every other recipient; that the recipients' e-mail addresses had been taken from the School's electronic gradebook; and that the School did not have the consent of the parents — the users of the respective e-mail addresses — for the described processing involving disclosure.

Article 4, paragraph 1, point 12 of the LPDP provides that the consent of the data subject is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her, while point 13 defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Article 5, paragraph 1, point 3 of the LPDP provides that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes of the processing ("data minimisation"), while paragraph 2 of the same Article provides that the Controller is responsible for compliance with paragraph 1 of that Article and must be able to demonstrate such compliance ("accountability").

Article 12, paragraph 1 of the LPDP provides that processing is lawful only if one of the following conditions is met: 1) the data subject has given consent to the processing of his or her personal data for one or more specifically defined purposes; 2) processing is necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into a contract; 3) processing is necessary for compliance with the Controller's legal obligations; 4) processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; 6) processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where the data subject is a minor.

Article 52 of the LPDP provides, inter alia, that the Controller must notify the Commissioner of any personal data breach that may pose a risk to the rights and freedoms of natural persons, without undue delay and, where feasible, within 72 hours after becoming aware of the breach.

In the present case, a personal data breach occurred within the meaning of Article 4, paragraph 1, point 13 of the LPDP, since the Controller made the e-mail addresses of all other recipients of the disputed messages available to each individual recipient, thereby also acting contrary to the principle of data minimisation set out in Article 5, paragraph 1, point 3 of the LPDP. Finally, the Controller failed to notify the Commissioner of the said personal data breach, which may entail a risk to the rights and freedoms of natural persons, although the Controller was obliged to do so in accordance with Article 52 of the LPDP.

When issuing this Warning, the Commissioner took into account the fact that the Controller, aware of the omission committed, promptly — and prior to the initiation of inspection supervision — adopted an internal act regulating in more detail the manner of electronic communication with parents.

072-21-2278/2025-07

1.4. Processing of minors' personal data made available on the Controller's official website

From the operative part:

It is PROHIBITED for PR AA Video Filming and Film Production _____, with its registered seat in Belgrade, at _____, as the personal data controller (hereinafter: the Controller), to make minors' personal data available through photographs on its official website for the purpose of sale.

The Controller is ORDERED to delete, within 5 days from the date of receipt of this decision, all photographs of minors published on the Controller's official website that were collected during dance events held in the Republic of Serbia for the purpose of sale, including sale via the official website, and to inform all potentially interested persons of the deletion of those data.

Part of the established factual situation:

- that the Controller's official website is available at the link _____;
- that the Controller has not appointed a data protection officer;
- that the Controller processes minors' personal data by taking photographs at dance tournaments held in the Republic of Serbia;
- that the Controller does not possess informed written consents for the processing of personal data;
- that the Controller does not have a legally binding act concluded with any organiser of dance tournaments;
- that every photograph featuring a minor is protected by a so-called "watermark";
- that the Controller does not have a Data Protection Impact Assessment; and
- that it is possible for any person to order photographs featuring minors which are available on the Controller's official website.

Action taken by the Controller:

The Controller informed the Commissioner that it had deleted all photographs taken at tournaments in the Republic of Serbia and had notified

all potentially interested persons thereof. It was established that, on its official website, the Controller informed all interested persons that, after 10 August 2025, the photographs taken during the 2024/25 season would be permanently deleted.

Case Number: 072-04-2368/2025-07

1.5. The Controller failed to protect the personal data of candidates for trainee positions and candidates for non-managerial posts contained in documents published on the Controller's website

From the operative part:

By processing the personal data of candidates for trainee positions and candidates for non-managerial posts (unique citizen identification numbers and residential addresses) contained in documents published on the Controller's website, the Controller infringed Article 5, paragraph 1, point 3) of the LPDP, because such processing was not adequate, relevant and limited to what was necessary in relation to the purpose of the processing ("data minimisation"); and Article 42, paragraph 2 of the LPDP, because the Controller failed, through the consistent application of appropriate technical, organisational and staffing measures, to ensure that only those personal data necessary for achieving each specific purpose of processing were processed.

From the reasoning:

In the course of the supervision procedure, it was established that, in the procedure for the recruitment of trainees and in the procedure conducted under the public competition for filling non-managerial posts, the Controller published on its website the ranking list for the recruitment of trainees and several decisions selecting candidates for non-managerial posts, without protecting (anonymising) the personal data of the candidates (unique citizen identification numbers and residential addresses).

In its submission, the Controller justified its actions by stating that "*the publication of the decisions and the ranking list was carried out on the basis of written declarations of consent given by all individuals concerned*".

We emphasise here that the consent of the data subject does not constitute an appropriate legal basis for most instances of personal data processing in the context of employment, including recruitment or the engagement of trainees, given that the employer–employee relationship is by its nature characterised by an imbalance of power between the two parties. Namely, the candidates' consent does not constitute a lawful basis for the processing concerned within the meaning of Articles 4, paragraph 1, point

12) and 15 of the LPDP, as it does not satisfy the conditions prescribed therein. Consequently, by conditioning individuals on giving consent, the Controller infringes Article 5, paragraph 1, point 1 of the LPDP, which concerns the lawfulness of processing.

We further emphasise that a declaration of will that is given *without the possibility of being modified or withdrawn without negative consequences for the individual's position* cannot be regarded as valid consent within the meaning of the LPDP. This is particularly important in cases involving the processing of personal data of candidates for employment and trainees by an employer, given that such candidates are in a position of subordination and imbalance vis-à-vis the employer.

We further point out that the data in question constitute personal data within the meaning of Article 4, point 1 of the LPDP, and *as such cannot be regarded as data relevant to the "transparency of the candidate selection process*", bearing in mind that personal data such as unique citizen identification numbers and residential addresses cannot affect the transparency of the selection process. Rather, the information relevant to transparency concerns the criteria that directly affect candidate selection — namely, the competencies assessed during the selection procedure, and the candidates' academic achievements and results of the entrance examination conducted by the Judicial Academy, as prescribed by the relevant by-laws. Therefore, the Controller's statement that "*the consent explicitly includes the right to publish data for the purpose of transparency of the candidate selection process… in line with the principles of public accessibility and transparency of the Controller's work*" is unfounded.

Taking into account the cited principles of personal data processing and the provisions of Article 42 of the LPDP, the Controller was obliged, when publishing the trainee ranking list and the decisions on the selection of candidates for non-managerial posts on its website for the purpose of conducting the recruitment procedure, to apply appropriate technical, organisational and staffing measures aimed at ensuring the effective application of personal data protection principles, such as data minimisation. The Controller was also required to ensure that only those personal data necessary for achieving each specific purpose of processing were processed, since, through the processing in question — namely the publication of all data contained in the ranking list and the decisions on candidates' selection — such data were made available to third parties, that is, to an unlimited number of natural persons.

In this regard, we emphasise that transparency in the selection of candidates for non-managerial posts and in the recruitment of trainees can be ensured through the methods prescribed by law, while at the same time protecting personal data (unique citizen identification numbers and residential addresses). By acting in such a manner, the Controller would have

complied with the principles set out in Article 5 of the LPDP, particularly the principles of data minimisation and purpose limitation.

Bearing in mind the provisions of the LPDP, and the fact that the Controller failed to protect (anonymise) the personal data (unique citizen identification numbers and residential addresses) of candidates for non-managerial posts and candidates for trainee positions contained in the ranking list and in the decisions on candidate selection published on the Controller's website during the recruitment procedure, it was established that the Controller infringed:

– the principle of "data minimisation" under Article 5, paragraph 1, point 3) of the LPDP, because such personal data were not adequate and limited to what was necessary in relation to the purpose of processing; and

– the provisions of Article 42, paragraphs 1 and 2 of the LPDP, concerning the availability of personal data, as a result of which a Warning was issued as a corrective measure, as set out in the operative part, and for the reasons stated above.

For the reasons set out, the Commissioner issued a Warning to the Controller.

Case Number: 072-04-23/2025-07

1.6. The Controller failed to protect the personal data contained in documents published on the Controller's official website under the sections "Public and Internal Competitions" and "Electronic Notice Board"

From the operative part:

By processing the personal data contained in documents published on the Controller's official website under the sections "Public and Internal Competitions" and "Electronic Notice Board", the Controller infringed:

Article 5, paragraph 1, point 3) of the LPDP, because such processing was not adequate, relevant and limited to what is necessary in relation to the purpose of the processing ("data minimisation"); and Article 42, paragraph 2 of the LPDP, because the Controller failed, through the consistent application of appropriate technical, organisational and staffing measures, to ensure that only those personal data necessary for achieving each specific purpose of processing were processed.

From the reasoning:

In the course of the supervision procedure, it was established that, on its website, under the public call for the allocation of non-repayable funds to households for the energy refurbishment of family houses and flats in

the territory of the City of X, the Controller published a List of households approved for funding under the energy refurbishment programme, which, in addition to the names and surnames of citizens, also contained their residential addresses.

It was further established during the supervision procedure that the Controller, under the "Electronic Notice Board" section of its website, published decisions and official letters when delivery by other means was not possible, and that, in doing so, the Controller failed to protect personal data that were not necessary for the purpose of such delivery (unique citizen identification numbers, names of parents, dates and places of birth, names and dates of birth of children, and other personal data relating to personal and civil status, including changes of personal name).

The Controller is reminded that, in accordance with Article 42 of the LPDP, it was obliged, when publishing documents on its website for the purpose of informing users about the outcome of proceedings, as well as when publishing documents for the purpose of public delivery, to apply appropriate technical, organisational and staffing measures aimed at ensuring the effective application of personal data protection principles, such as data minimisation. The Controller was also required to ensure that only those personal data necessary for achieving each specific purpose of processing were processed, given that, through the processing in question — namely the publication of all data contained in the relevant documents — such data were made available to third parties, that is, to an unlimited number of natural persons.

In the present case, the purpose of the processing could also have been achieved by other means posing *a lesser risk to individuals' privacy*, namely by protecting (anonymising) personal data. By acting in such a manner, the Controller would have complied with the principles set out in Article 5 of the LPDP, particularly the principles of data minimisation and purpose limitation.

Bearing in mind the provisions of the LPDP and the fact that the Controller failed to protect (anonymise) personal data in the documents published on the Controller's website in the procedure for allocating non-repayable funds to households for the energy refurbishment of family houses and flats in the territory of the City of X, as well as in the procedure of public delivery of documents where delivery by other means was not possible, it was established that the Controller infringed:

- the principle of "data minimisation" under Article 5, paragraph 1, point 3) of the LPDP, because such personal data were not adequate and limited to what was necessary in relation to the purpose of the processing; and
- the provisions of Article 42, paragraphs 1 and 2 of the LPDP, concerning the availability of personal data, as a result of which a Warning

was issued as a corrective measure, as set out in the operative part, and for the reasons elaborated above.

For the reasons stated, the Commissioner issued a Warning to the Controller.

Case Number: 072-04-170/2025-07

1.7. The Controller failed to apply appropriate technical, organisational and staffing measures for the protection of personal data when delivering/publishing documents on the notice board

From the operative part:

A WARNING is issued to the Controller because, when publishing documents on the notice board that contain personal data, the Controller fails to implement appropriate technical, organisational and staffing measures for the protection of personal data, in accordance with Article 42 of the LPDP, with a view to preserving their integrity and confidentiality, in accordance with Article 5, paragraph 1, point 6) of the LPDP, thereby jeopardising the security of personal data and the purpose of their processing.

Part of the established factual situation:

The Controller stated that it "did not effect delivery via the notice board because it knew that delivery had already been effected by registered mail, which was indicated and documented by the proof relating to the tracking of the postal item (Track Your Item – Postal Service)", and further that "the notice board referred to as evidence is used solely for the internal needs of the management", and that "the Controller, as employer, was not aware that those acts were placed on the notice board, nor that they had been posted there by persons not authorised to do so, solely for the purpose of photographing those acts and submitting a report to the Commissioner". The Controller also stated that "delivery had been carried out in accordance with the Labour Law, by sending via registered mail, and that delivery via publication on the Controller's notice board had not taken place".

During the supervision, the Commissioner's authorised officers photographed the notice boards, on which it was established that the acts in question — the Warning to the employee regarding the existence of grounds for termination of the employment contract — were not posted.

In relation to the established facts and the circumstances of the case, the Commissioner issued a Warning for the following reasons.

The principles of personal data processing are laid down in Article 5, paragraph 1 of the LPDP.

Article 12 of the LPDP provides that processing is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes; 2) processing is necessary for the performance of a contract to which the data subject is a party or for taking steps, at the request of the data subject, prior to entering into a contract; 3) processing is necessary for compliance with the Controller's legal obligations; 4) processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; 6) processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where the data subject is a minor.

Article 42, paragraphs 1–3 of the LPDP provide that, taking account of the state of technological development and the cost of implementation, the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons arising from the processing, the Controller, when determining the manner of processing and throughout the processing, must: 1) apply appropriate technical, organisational and staffing measures, such as pseudonymisation, aimed at ensuring the effective application of personal data protection principles, such as data minimisation; 2) ensure the application of the necessary safeguards during the processing, in order to meet the processing conditions prescribed by this Law and protect the rights and freedoms of data subjects. The Controller must, through the consistent application of appropriate technical, organisational and staffing measures, ensure that only those personal data necessary for achieving each specific purpose of processing are processed at all times. This obligation applies to the quantity of data collected, the scope of their processing, the duration of their storage and their accessibility. The measures referred to in paragraph 2 must always ensure that, without the participation of a natural person, personal data cannot be made available to an unlimited number of natural persons.

Furthermore, Article 50 of the LPDP provides that, taking account of the state of technological development and the cost of implementation, as well as the nature, scope, circumstances and purpose of the processing, and the likelihood and severity of the risk to the rights and freedoms of natural persons, the Controller and the Processor must implement appropriate technical, organisational and staffing measures in order to achieve a level of security appropriate to the risk.

The LPDP also prescribes that, in the field of labour and employment, the provisions of the laws governing labour and employment and the

provisions of collective agreements apply to the processing of personal data, together with the application of the provisions of the LPDP (Article 91 of the LPDP).

In this regard, Article 180 of the Labour Law ("Official Gazette of the Republic of Serbia", Nos. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – Constitutional Court decision, 113/2017 and 95/2018 – authentic interpretation) prescribes that, prior to terminating an employment contract in the cases referred to in Article 179, paragraphs 2 and 3 of that Law, the employer must warn the employee in writing of the existence of grounds for termination of the employment contract and allow the employee a period of at least eight days from the date of delivery of the warning to respond to the allegations set out therein.

In this regard, Article 185 of the Labour Law provides that an employment contract is terminated by a written decision, which must contain a statement of reasons and information on legal remedies. The decision must be delivered to the employee personally, on the employer's premises, or to the employee's place of residence or domicile. If the employer is unable to deliver the decision in the manner prescribed in paragraph 2 of this Article, the employer must draw up a written record of that fact. In the situation referred to in paragraph 3 of this Article, the decision is posted on the employer's notice board and is deemed to have been delivered upon the expiry of eight days from the date of posting. The employee's employment terminates on the date of delivery of the decision, unless another date is prescribed by this Law or specified in the decision. The employee must inform the employer in writing, on the next day after receiving the decision, if he or she wishes to resolve the dispute before an arbitrator in accordance with Article 194 of this Law.

Having regard to the above, since the Commissioner could not establish with certainty that, in the present case, the Controller had processed personal data in a manner contrary to the provisions of the LPDP and the Labour Law, but did establish that the Controller, when publishing and delivering documents via the notice board — which constitutes a means of effecting delivery within the meaning of the Labour Law and which is physically accessible to a wider circle of persons due to the lack of secured access — failed to implement appropriate technical, organisational and staffing measures for protection, in accordance with Article 42 of the LPDP, to ensure the integrity and confidentiality of the personal data contained in those documents, thereby jeopardising both the purpose of the processing and the protection of the personal data of the individuals to whom the data relate, contained in the documents concerned.

Case Number: 072-21-3206/2025-07 и 072-21-3151/2025-07

1.8. Processing of employees' personal data through publication in a Viber group and on the institution's notice board

From the operative part:

The Commissioner issued a Warning to Secondary School X, as the personal data controller, because by processing personal data — namely, by publicly disclosing the personal data of employees and members of their families via a *Viber* group and the institution's notice board — it infringed the principle of "lawfulness, fairness and transparency" under Article 5, paragraph 1, point 1 of the LPDP, the principle of "data minimisation" under Article 5, paragraph 1, point 3, and the principle of "integrity and confidentiality" under Article 5, paragraph 1, point 6 of that Law.

From the reasoning:

In the course of the supervision procedure, it was established, inter alia, that the School Secretary published, on the School's notice board and in the *Viber* group comprising all School employees, a document of the National Health Insurance Fund containing the names, surnames, unique citizen identification numbers (JMBG) and health insurance numbers (LBO) of a total of 70 employees and members of their families who are insurance beneficiaries.

Article 5, paragraph 1, point 1 of the LPDP prescribes that personal data must be processed lawfully, fairly and transparently in relation to the data subject ("lawfulness, fairness and transparency"), and that processing is lawful when carried out in accordance with this Law or another law governing processing. Point 3 of the same Article prescribes that personal data must be adequate, relevant and limited to what is necessary in relation to the purpose of the processing ("data minimisation"). Point 6 of the same Article prescribes that personal data must be processed in a manner ensuring appropriate protection of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by applying appropriate technical, organisational and staffing measures ("integrity and confidentiality").

Article 12, paragraph 1 of the LPDP prescribes that processing is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes; 2) processing is necessary for the performance of a contract to which the data subject is a party or for taking steps, at the request of the data subject, prior to entering into a contract; 3) processing is necessary for compliance with the Controller's legal obligations; 4) processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; 6) processing is necessary for

the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring personal data protection, particularly where the data subject is a minor.

The Controller was informed that, by processing personal data—namely, by publicly disclosing via the *Viber* group the personal data of employees and members of their families—it had infringed the principle of "lawfulness, fairness and transparency", because the said data were disclosed without a lawful basis; the principle of "data minimisation", because such personal data were not adequate, relevant and limited to what was necessary in relation to the purpose of the processing; and the principle of "integrity and confidentiality", because the personal data were not processed in a manner ensuring appropriate protection, including protection against unauthorised or unlawful processing, through the application of appropriate technical, organisational and staffing measures.

Case Number: 072-21-2825/2024-07

1.9. Failure to implement appropriate technical, organisational and staffing measures for the protection of employees' personal data

From the operative part:

A WARNING is issued to the Controller because it entered personal data of its employees — including the personal data of the complainant — into an electronic register, and subsequently entered into that register all employee-related documentation submitted to the Controller, without an appropriate legal basis for doing so and without informing the employees of the processing in the manner prescribed by the LPDP. Moreover, the Controller failed to carry out, prior to processing, any testing, assessment, or evaluation of the effectiveness of the technical, organisational and staffing measures for the security of processing, taking into account the state of technological development and the cost of implementation, as well as the nature, scope, circumstances and purpose of the processing, and the likelihood and severity of risks to the rights and freedoms of natural persons, in order to achieve a level of security appropriate to the risk. As a result, employees' personal data were made accessible to unauthorised employees and other engaged persons, whereby the Controller infringed the provisions of Articles 5, paragraph 1, points 1) and 6), 12, 42, paragraph 1, point 2), and 50 of the LPDP.

Part of the established factual situation:

In the course of the inspection supervision procedure, it was established, inter alia, that the Controller maintains records of its work and doc-

umentation in electronic form – in a register; that the Controller entered into the register the personal data of its employees, including the personal data of the complainant; that, according to the Controller's representatives, employees were orally informed that their data had been entered into the register; that all documentation generated in the Controller's work, or submitted to the Controller concerning employees, was entered into the register for employees from the moment the employees were recorded in the register; that, in relation to the documents referred to in the complaint, which concern enforcement proceedings conducted against an employee, the Controller opened files No. .., No. .. and No. .., and that the documents were scanned and entered into the register; that, according to the statements of the Controller's representatives, even though individual user accounts had been created, all employees who have an account for accessing the data in the register are able to access the personal data of employees entered therein, and that the application does not allow the Controller to define access privileges for each user individually; and that the Controller has no possibility of monitoring employees' log-ins.

Article 5, paragraph 1 of the LPDP lays down the principles of personal data processing, prescribing that personal data must be: processed lawfully, fairly and transparently in relation to the data subject, and that processing is lawful when carried out in accordance with this Law or another law governing processing ("*lawfulness, fairness and transparency*"); collected for purposes that are specifically defined, explicit, justified and lawful, and not further processed in a manner incompatible with those purposes ("*purpose limitation*"); adequate, relevant and limited to what is necessary in relation to the purpose of the processing ("*data minimisation*"); accurate and, where necessary, kept up to date, with all reasonable steps taken to ensure that inaccurate personal data are erased or rectified without delay ("*accuracy*"); stored in a form which permits identification of data subjects for no longer than is necessary for the purposes of the processing ("*storage limitation*"); processed in a manner that ensures appropriate protection of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, through the application of appropriate technical, organisational and staffing measures ("*integrity and confidentiality*"). In accordance with paragraph 2 of this Article of the LPDP, the Controller is responsible for compliance with the provisions of paragraph 1 of this Article and must be able to demonstrate such compliance ("*accountability*").

Article 12, paragraph 1 of the LPDP prescribes that the processing of personal data is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes; 2) the processing is necessary for the performance of a contract to which the data subject is a party, or for taking steps,

at the request of the data subject, prior to entering into a contract; 3) the processing is necessary for compliance with the Controller's legal obligations; 4) the processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; 6) the processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where the data subject is a minor.

Article 42, paragraph 1, point 2) of the LPDP prescribes that, taking into account the state of technological development and the cost of implementation, the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons arising from the processing, the Controller, when determining the manner of processing and throughout the processing, must ensure the application of the necessary safeguards, in order to meet the processing conditions prescribed by this Law and to protect the rights and freedoms of the data subjects.

Article 50, paragraphs 1 and 2 of the LPDP prescribe, inter alia, that—taking into account the state of technological development and the cost of implementation, as well as the nature, scope, circumstances and purpose of the processing, and the likelihood and level of risk to the rights and freedoms of natural persons—the Controller must implement appropriate technical, organisational and staffing measures in order to achieve a level of security appropriate to the risk, and that, where necessary, those measures shall include, inter alia, a procedure for the regular testing, assessment and evaluation of the effectiveness of the technical, organisational and staffing measures for the security of processing. Paragraph 3 of this Article prescribes that, when assessing the appropriate level of security referred to in paragraph 1, particular account shall be taken of the risks posed by the processing, and in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Based on the facts established during the inspection supervision procedure, it was determined that the Controller acted in contravention of the principle of lawfulness, fairness and transparency set out in Article 5, paragraph 1, point 1) of the LPDP, which requires that personal data be processed *lawfully*, fairly and transparently in relation to the data subject, and that *processing is lawful only when carried out in accordance with this Law or another law governing processing*. Specifically, the Controller entered the personal data of employees, including the personal data of the complainant, into the electronic register, despite having no legal basis for doing so.

The Controller did not provide employees whose personal data were entered into the User Register with the information required under Articles 23 and 24 of the LPDP, in the manner prescribed by those provisions. Specifically, during the supervision procedure the Controller stated that employees had been orally informed of the entry of their data into the User Register, which is not compliant with Article 21 of the LPDP, prescribing that the information referred to in Articles 23 and 24 must be provided in writing, including in electronic form where appropriate. In addition, it was established that the Controller had infringed Article 5, paragraph 1, point 6) of the LPDP — *the principle of integrity and confidentiality* — as well as Articles 42, paragraph 1, point 2), and 50, paragraph 2, point 4) of the LPDP, because, prior to entering employees' personal data into the User Register, the Controller failed to conduct any testing, assessment or evaluation of the effectiveness of the technical, organisational and staffing measures for the security of processing, nor did it ensure, during the course of the processing, the application of the necessary protective mechanisms to safeguard the rights and freedoms of the data subjects. Consequently, these personal data were made accessible to unauthorised persons. The Controller failed to recognise that the access rights of authorised staff to the personal data of employees entered into the User Register were not restricted and failed to protect the entered data from unauthorised processing by implementing appropriate organisational and staffing measures for personal data protection, which could have reduced the risk of unauthorised disclosure to the lowest possible level. It is undisputed that all three submissions, in respect of which files No. …, No. … and No. … were created, were addressed to the Controller on the envelope, and that the Controller was authorised to record them and act upon them in accordance with the Law on General Administrative Procedure, the Labour Law and the Law on Enforcement and Security. However, the authority to record a submission and process personal data for the purpose of fulfilling the Controller's legal obligations does not include the authority to make employees' personal data accessible to unauthorised persons — particularly bearing in mind that the data entered into the register can be accessed by a significantly wider group of individuals than those who would have access to the data had they not been entered into the register. This applies all the more given that the data concern the personal circumstances of the complainant, are not related to the work of the Controller, and are not required by the Controller's employees who, by virtue of their entry into the register, gained access to them for the performance of their duties.

The Commissioner also took into account the fact that employees, in accordance with the provisions of … and the Controller's internal acts, had been informed that any information and data they became aware of were to be treated as official secrets, and that they were obliged to keep such

data confidential. However, the Commissioner assessed that this fact had no bearing on the decision, given that under the LPDP the Controller is obliged, when determining the manner of processing and throughout the processing, to ensure the application of the necessary protective mechanisms in order to safeguard the rights and freedoms of data subjects from unauthorised disclosure and unauthorised access. Furthermore, in accordance with the LPDP, the Controller remains responsible for any personal data breach caused by its employees, even where such employees acted contrary to instructions. This position is also confirmed in the case law of the European Court of Justice (Case C-741/21, GP v juris GmbH).

Action taken by the Controller:

The Controller submitted a communication informing the Commissioner, inter alia, that the documents which had given rise to the initiation of the inspection supervision procedure had been removed from the register; that the Controller had adopted Instructions and work orders governing the processing, storage and access to personal data, as well as the responsibilities of employees within the work process; that employees had signed a confidentiality statement confirming that they were aware of their obligation to maintain the confidentiality of all personal data, especially data not necessary for the performance of their official duties; that the Controller would continue to provide regular training and awareness-raising for employees regarding their obligations in the field of personal data protection, as well as periodic checks of the implementation of technical and organisational measures; and that the documents relating to the cases which triggered the inspection supervision procedure had been removed from the register.

Case Number: 072-21-2481/2025-07

1.10. Application of personal data protection measures when delivering a pupil's pedagogical documentation to a parent

From the operative part:

The Commissioner issued a warning to Primary School X, as the Controller, because it had not regulated the delivery of a pupil's pedagogical documentation to a parent in a manner ensuring adequate protection against unauthorised or unlawful processing, as well as against accidental loss, destruction or damage. The school failed to implement appropriate technical, organisational and staffing measures to achieve a level of security appropriate to the risk, thereby infringing Article 5, paragraph 1, point 6 of the LPDP and Article 50 of the same Law.

From the reasoning:

In the course of the supervision procedure, it was established, inter alia, that the Controller had not regulated, by any act, the method for delivering a pupil's pedagogical documentation to a parent, but that such delivery was carried out on the basis of established practice and internal arrangements between teachers and parents; that, whenever possible, the documentation was delivered to the parent in person; and that, in individual cases and in agreement with the parent, the documentation was delivered in the manner considered most efficient and convenient in the given circumstances — by e-mail, in person, or via a personal assistant.

Article 4, paragraph 1, point 1 of the LPDP prescribes that personal data are any information relating to an identified or identifiable natural person, directly or indirectly, particularly by reference to an identifier such as a name, identification number, location data, an online identifier, or one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural or social identity.

Point 3 of the same paragraph prescribes that the processing of personal data means any operation or set of operations performed on personal data, such as collection, recording, sorting, grouping, structuring, storage, adaptation or alteration, disclosure, access, use, disclosure by transmission or delivery, copying, dissemination or otherwise making available, alignment, restriction, erasure or destruction.

Article 5, paragraph 1, point 6 of the LPDP prescribes that personal data must be processed in a manner that ensures appropriate protection, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, through the application of appropriate technical, organisational and staffing measures ("integrity and confidentiality"). Paragraph 2 of the same Article prescribes that the Controller is responsible for compliance with the provisions of paragraph 1 and must be able to demonstrate such compliance ("accountability").

Article 50, paragraph 1 of the LPDP, which regulates the security of processing, prescribes that—taking into account the state of technological development and the cost of implementation, as well as the nature, scope, circumstances and purpose of the processing, and the likelihood and severity of risks to the rights and freedoms of natural persons—the Controller and processor must implement appropriate technical, organisational and staffing measures in order to achieve a level of security appropriate to the risk. Paragraph 2, point 1 of the same Article prescribes that, where necessary, the measures referred to in paragraph 1 shall particularly include the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Paragraph 3 prescribes that, when assessing the appropriate level of security referred to in paragraph 1, particular account shall be taken of the risks arising from processing,

especially the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Article 15, paragraph 5 of the Law on the Fundamentals of the Education System ("Official Gazette of the RS", Nos. 88/2017, 27/2018 – amended, 10/2019, 27/2018 – amended, 6/2020, 129/2021, 92/2023 and 19/2025; hereinafter: the LFES) prescribes that all forms of collection, processing, publication and use of data shall be carried out in accordance with that Law, special laws, and the law governing the protection of personal data.

Article 76, paragraph 3 of the LFES prescribes that the Individual Education Plan (hereinafter: IEP) is a special act aimed at ensuring the optimal development of the child or pupil and the achievement of educational outcomes, in accordance with prescribed goals and principles, that is, the satisfaction of the educational needs of the child or pupil. Paragraph 4 of the same Article prescribes that the IEP is prepared by the team for additional support to the child or pupil, in cooperation with the parent or other legal representative, on the basis of previously implemented, recorded and evaluated individualisation measures and the prepared pedagogical profile of the child, pupil or adult, and that it is implemented following the parent's or legal representative's consent.

Article 184, paragraph 1 of the LFES prescribes that an institution, a higher education institution, an institution for pupil and student standard, or a publicly recognised organiser of activities, shall ensure measures protecting against unauthorised access to and use of data contained in the records it maintains.

Article 3, paragraph 5 of the Rulebook on the Assessment of Pupils in Primary Education ("Official Gazette of the RS", No. 10/2024; hereinafter: the Rulebook on Assessment) prescribes, inter alia, that formative assessments are, as a rule, recorded in the teacher's pedagogical documentation, in electronic and/or written form, in accordance with this Rulebook, and most often relate to the regular monitoring of a pupil's progress and achievement, the manner in which the pupil learns, the degree of independence in work, the manner of cooperation with other pupils in the learning process, and other data relevant for monitoring the pupil. Paragraph 6 of the same Article prescribes that pedagogical documentation means documentation kept in electronic and/or written form, and that it contains personal data on the pupil and his or her individual characteristics relevant to achievement, data on achievement checks, pupil engagement and progress, recommendations given, pupil behaviour, and other data relevant for working with the pupil and for his or her progress.

Article 21 of the Rulebook on Assessment prescribes that, in the assessment procedure, the teacher collects and records data on the pupil's achievement, learning process, progress and development during the school year in the prescribed records and in the pedagogical documentation referred to in Article 3, paragraph 6 of this Rulebook, and that the data entered in the pedagogical documentation are used to inform parents when deciding on a complaint or appeal against a mark, as well as in the process of self-evaluation and external evaluation of the quality of the institution's work.

Article 12 of the Professional Guidance on the Method of Preparing School Documentation, No. 119-01-346/1/2014-01 of 27 August 2014, prescribes that: pedagogical documentation constitutes the teacher's personal record containing data significant for work with the pupil and for the pupil's progress; the scope and structure of the pedagogical documentation are determined by the teacher on the basis of his or her professional competences and the specificities of the subject (formative and summative assessment and other data the teacher considers necessary); there is no prescribed template for pedagogical documentation; and such documentation may be kept in electronic or paper form.

Having regard to the cited provisions of the LPDP relating to the principle of integrity and confidentiality and to processing security, as well as the relevant provisions of the LFES and the cited by-laws, it was established that the Controller had not applied, in accordance with the state of technological development and the cost of implementation, and taking into account the nature, scope, circumstances and purpose of the processing, as well as the likelihood and severity of risks to the rights and freedoms of natural persons, appropriate technical, organisational and staffing measures regarding the manner in which a pupil's pedagogical documentation is delivered to a parent. As a result, the personal data contained in the pedagogical documentation were not processed in a manner ensuring appropriate protection, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, thereby infringing the principle of integrity and confidentiality under Article 5, paragraph 1, point 6 of the LPDP, as well as Article 50 of the same Law. In relation to the above, the Controller is expressly reminded that, where the processing operation (in this case, the manner of delivering a pupil's pedagogical profile to a parent) is not prescribed by a special law, it is obliged, when undertaking such processing of personal data, to apply the principles and provisions of the LPDP.

Case Number: 072-21-2337/2024-07

1.11. Misuse by an employee of a record containing personal data, maintained by the Controller in accordance with the law

From the operative part:

A WARNING is issued to the Controller because it has infringed:

– the principle of integrity and confidentiality, as the personal data were made accessible to an unknown number of individuals and were not processed in a manner ensuring appropriate protection, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, through the application of appropriate technical, organisational and staffing measures; and
– the provisions of Article 42, paragraphs 1 and 2 of the LPDP concerning the accessibility of personal data, for which reason a warning has been imposed as a corrective measure, as set out in the operative part, with the reasoning provided above.

Part of the established factual situation:

– That on 13 March 2025 the Controller submitted to the Commissioner a Notification of a Personal Data Breach;
– That the Controller is aware which employee accessed the personal data — specifically, the personal data of AA and BB — on the basis of the available log files, i.e., by identifying the user account and password through which access to these individuals' personal data was obtained;
– That the Controller's representatives stated that a personal data breach of this nature had never occurred before, and that in December 2024 a total of 1,643 employees completed information security training at the National Academy for Public Administration;
– That the Controller has adopted a Rulebook on Personal Data Protection, and that all persons engaged by the Controller sign a Confidentiality and Non-Disclosure Statement and a Confidentiality and Non-Disclosure Agreement; and
– That the Controller has prepared a Proposal to initiate a procedure for determining the responsibility of the employee following the personal data breach.

Action taken by the Controller:

The Controller informed the Commissioner that, in addition to initiating disciplinary proceedings against the employee who was found to have accessed the personal data of the individuals referred to in the report, it had shortened the computer auto-lock time due to user inactivity to five minutes and had introduced continuous training for employees.

Case Number: 072-04-2484/2025-07

1.12. Personal Data Minimisation

From the operative part:

A WARNING is issued to the Controller because it failed to implement appropriate technical, organisational and staffing measures and failed to apply personal data minimisation, thereby infringing:

- the principle of personal data minimisation under Article 5, paragraph 1, point 3 of the LPDP, which requires that personal data be adequate, relevant and limited to what is necessary in relation to the purpose of the processing;
- the principle of integrity and confidentiality under Article 5, paragraph 1, point 6 of the LPDP, which requires that personal data be processed in a manner ensuring appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, through the application of appropriate technical, organisational and staffing measures;
- the provisions of Article 42, paragraphs 1 and 2 of the LPDP, which prescribe that the Controller must implement appropriate technical, organisational and staffing measures to ensure that processing is carried out in accordance with the LPDP and be able to demonstrate such compliance, taking into account the nature, scope, circumstances and purpose of the processing, as well as the likelihood and severity of risks to the rights and freedoms of natural persons; and that such measures must be reviewed and updated where necessary.

Part of the established factual situation:

The Commissioner received a Complaint concerning a personal data breach, stating, inter alia, that on the Controller's official website, a publicly accessible document was available containing personal data of teaching and non-teaching staff, including their Unique Master Citizen Numbers (JMBG). The Controller indicated that, as a remedial measure, "the document was removed and a revised version was uploaded, with personal data removed as excessive processing of personal data."

The principles of personal data processing are prescribed by Article 5, paragraph 1 of the Law on Personal Data Protection, under which personal data must: 1) be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"). Lawful processing is processing carried out in accordance with this Law or another law governing processing; 2) be collected for purposes that are specifically determined, explicit, justified and lawful, and must not be further processed in a manner incompatible with those purposes ("purpose limitation"); 3) be adequate, relevant and limited to what is necessary in

relation to the purpose of the processing ("data minimisation"); 4) be accurate and, where necessary, kept up to date. Taking into account the purpose of the processing, all reasonable measures must be taken to ensure that inaccurate personal data are erased or rectified without delay ("accuracy"); 5) be kept in a form which permits identification of the data subject for no longer than is necessary for the purpose of the processing ("storage limitation"); 6) be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, as well as against accidental loss, destruction or damage, by applying appropriate technical, organisational and personnel measures ("integrity and confidentiality"). Article 5, paragraph 2 of the Law prescribes that the controller is responsible for complying with the provisions of paragraph 1 of this Article and must be able to demonstrate such compliance ("accountability").

Pursuant to Article 42, paragraph 1 of the Law on Personal Data Protection, taking into account the level of technological development and the costs of its implementation, the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons arising from the processing, the controller is, when determining the manner of processing and during the processing itself, obliged to: apply appropriate technical, organisational and personnel measures, such as pseudonymisation, aimed at ensuring effective application of the personal data protection principles, such as data minimisation; and ensure the application of the necessary protection mechanisms during the processing, in order to meet the conditions for processing prescribed by this Law and to protect the rights and freedoms of the data subjects. The controller is obliged, through continuous application of appropriate technical, organisational and personnel measures, to ensure that only those personal data which are necessary for achieving each individual purpose of the processing are processed at all times, and that this obligation applies to the amount of data collected, the scope of the processing, the period of their storage and their accessibility, as prescribed by paragraph 2 of the cited Article.

Having regard to the above, and to the fact that a personal data breach occurred at the controller, the Commissioner issued this warning. Namely, by acting in such a manner, the controller failed to apply the principle of "data minimisation" and the principle of "integrity and confidentiality", that is, failed to apply a minimisation process that would reduce the likelihood of a personal data breach occurring. By doing so, the controller endangered the confidentiality of personal data within the meaning of the principle of "integrity and confidentiality" under Article 5, paragraph 1, point 6) of the Law, which requires that personal data must be stored and processed in a manner that ensures their protection against further unauthorised processing.

Action taken by the Controller:

Following the issuance of the Warning, on 28 May 2025 the controller removed the document from the website and uploaded a new, amended document; the controller will continue to conduct regular training of employees in order to prevent any recurrence of violations of the provisions of the Law on Personal Data Protection.

Case Number: 072-04-3152/2025-07

1.13. Implementation of Appropriate Technical, Organisational and Staffing Measures in the Storage of Archived Patients' Medical Documentation

From the operative part:

The Commissioner issued a warning to Healthcare Institution X, as the controller, because it does not store patients' medical documentation in a manner that ensures adequate protection of personal data, including protection from unauthorised or unlawful processing, as well as from accidental loss, destruction or damage. The controller also fails to implement appropriate technical, organisational and personnel measures to achieve an adequate level of security in relation to the risk, thereby violating Article 5(1)(6) of the Law on Personal Data Protection and Article 50 of the same Law.

From the reasoning:

During the supervisory inspection procedure, it was established, inter alia, that the Controller stores archived medical documentation created in the course of performing its activities — including medical records, hospital treatment histories, medical reports, laboratory findings, biological samples for pathohistological analyses, and other such records — in a facility that is not adequately secured. As a result, the medical documentation in question is exposed both to the risk of unlawful access and to exposure to precipitation and other weather conditions.

Article 4 of the Law on Personal Data Protection stipulates, inter alia, that the processing of personal data means any operation or set of operations performed on personal data, such as collection, recording, sorting, grouping or structuring, storage, adaptation or alteration, disclosure, access, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, comparison, restriction, erasure, or destruction; that health data constitute data concerning the physical or mental health of a natural person, including data relating to the provision of healthcare services, which reveal information about that person's health status.

Article 5(1)(6) of the Law on Personal Data Protection prescribes that personal data must be processed in a manner ensuring appropriate protection of personal data, including protection against unauthorised or unlawful processing, as well as against accidental loss, destruction or damage, through the application of appropriate technical, organisational and staffing measures ("integrity and confidentiality"). Paragraph 2 of the same Article stipulates that the Controller is responsible for applying the provisions of paragraph 1 and must be able to demonstrate such compliance ("accountability").

Article 50(1) of the Law on Personal Data Protection prescribes that, in accordance with the level of technological development and the costs of its implementation, the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons arising from the processing, the Controller and the Processor shall implement appropriate technical, organisational and staffing measures in order to achieve an adequate level of security relative to the risk. Paragraph 3 stipulates that, when assessing the appropriate level of security referred to in paragraph 1 of this Article, particular account shall be taken of the risks of the processing, especially the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data that are transmitted, stored or otherwise processed.

Article 54(3) of the Health Care Act ("Official Gazette of the RS", Nos. 25/2019, 92/2023 – authentic interpretation, and 29/2025 – Constitutional Court decision) prescribes that healthcare institutions and private practices are obliged to protect patients' medical documentation from unauthorised access, copying and misuse, regardless of the form in which the data from the medical documentation are stored, in accordance with the law on patients' rights and the law governing healthcare documentation and records in the field of health.

Article 21(1) of the Law on Patients' Rights ("Official Gazette of the RS", Nos. 45/2013 and 25/2019 – other law) prescribes that data on a patient's health status, i.e. data contained in medical documentation, constitute personal data and represent particularly sensitive personal data of the patient, in accordance with the law.

Article 7 of the Law on Healthcare Documentation and Records in the Field of Health ("Official Gazette of the RS", No. 92/2023; hereinafter: the LHDH) prescribes that personal data contained in medical and healthcare documentation shall be processed in accordance with this Law, other laws governing the processing of personal data, as well as the law governing personal data protection.

Article 38 of the LHDH prescribes that data from a patient's medical documentation constitute a special category of personal data, and

that healthcare institutions, private practices and other legal entities are obliged to collect and process personal data of patients in a manner that ensures the exercise of the right to privacy and the right to confidentiality of the patient's personal data, in accordance with the law governing patients' rights and the law governing personal data protection.

Article 52(1) of the LHDH prescribes that the processing of personal data contained in healthcare documentation and records shall be carried out in accordance with the law governing personal data protection. Paragraph 2 of the same Article, inter alia, prescribes that healthcare institutions, as well as authorised healthcare professionals, healthcare associates and other authorised persons who keep medical documentation and records in accordance with this Law and the regulations adopted for its implementation, are obliged to protect medical documentation and patients' records from unauthorised access, inspection, copying and misuse, irrespective of the form in which the data from the medical documentation are stored.

Article 53 of the LHDH prescribes that healthcare institutions, private practices and other legal entities are obliged to establish and maintain a security system that includes measures to ensure the security of the data they hold, in accordance with this Law, the Law on Information Security, ISO standards, and the law governing personal data protection.

Having regard to the provisions of the Law on Personal Data Protection concerning the principle of "integrity and confidentiality", as well as the provisions of the Law on Healthcare Protection and the Law on Healthcare Documentation and Records relating to the storage of patients' medical documentation, it was established that the Controller did not, in accordance with the level of technological development and the costs of its implementation, the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons, apply appropriate technical, organisational and staffing measures in relation to the storage of patients' healthcare documentation. Consequently, the personal data contained in the relevant healthcare documentation were not processed in a manner that ensures adequate protection of personal data, including protection from unauthorised or unlawful processing, as well as from accidental loss, destruction or damage, thereby violating the principle of "integrity and confidentiality" set out in Article 5(1)(6) of the Law on Personal Data Protection and Article 50 of the same Law.

Case Number: 072-04-2546/2024-07

1.14. The Controller unlawfully accessed a patient's medical record within its medical information system

From the operative part:

The Commissioner issued a Warning to the Primary Healthcare Centre (hereinafter: the Controller), as it processed patients' personal data contained in the medical information system contrary to Article 5(1)(1) of the Law on Personal Data Protection (LPDP), namely contrary to the principle of "lawfulness, fairness and transparency", by accessing health data without a legal basis under Article 47 of the Law on Health Documentation and Records in the Field of Healthcare ("Official Gazette of the RS", No. 92/2023; hereinafter: the LHDH), which regulates the right of access to data from a patient's e-record, thereby also infringing Article 17 of the LPDP; contrary to Article 5(1)(6) of the LPDP, namely the principle of "integrity and confidentiality", as it did not process the patient's personal data in a manner that ensures adequate protection of personal data, including protection against unauthorised or unlawful processing through the application of appropriate technical, organisational and personnel measures; and contrary to Article 42 of the LPDP, as it failed, when determining the manner of processing and during the processing of patients' personal data, to ensure the application of the necessary safeguards during the processing in order to meet the conditions for processing prescribed by this Law and to protect the rights and freedoms of the data subjects, and failed to ensure, through the continual application of appropriate technical, organisational and personnel measures, that only the personal data necessary for achieving each specific purpose of processing are processed, such obligation applying to the quantity of data collected, the scope of processing, the retention period and their accessibility.

From the reasoning:

It was established that the Controller, contrary to its obligation under Article 53 of the Law on Health Documentation and Records in the Field of Healthcare (LHDH), had neither established nor maintained a security system incorporating measures to ensure the security of data in accordance with that Law, the Law on Information Security, ISO standards, and the Law governing the protection of personal data.

Given that the supervisory procedure established that access to and viewing of health data in the health information system was, by default, enabled to all healthcare professionals for every patient, it was determined that the Controller, by processing the patient's data in this manner, had infringed the principle of "integrity and confidentiality" of personal data

under Article 5(1)(6) of the Law on Personal Data Protection (LPDP), as well as Article 42(1)(2) and Article 42(2) of the LPDP. The Controller failed, when determining the manner of processing and during the processing of patients' personal data, to ensure the application of the necessary safeguards during processing so as to meet the conditions for processing prescribed by this Law and to protect the rights and freedoms of the data subjects. Furthermore, by failing to continually apply appropriate technical, organisational and personnel measures, the Controller did not ensure that only those personal data necessary for achieving each specific purpose of processing were processed, such obligation applying to the amount of data collected, the scope of processing, the retention period and the accessibility of the data.

Taking into account the provisions of the LPDP, as well as the provisions of the other regulations cited in this warning, and on the basis of the evidence submitted by the complainant, it was established that the Controller accessed her health data contrary to Article 47 of the Law on Health Documentation and Records in the Field of Healthcare, thereby infringing Article 5(1)(1) of the LPDP, namely the principle of "lawfulness, fairness and transparency", as well as the provisions of Article 17 of the LPDP.

Action taken by the Controller:

In the further course of the proceedings, within the 15-day time limit from the date of receipt of the Warning, the Controller submitted a statement indicating that the necessary measures had been taken in order to remedy the established infringements of the LPDP, namely that a new medical information system had begun to be used, under which, in accordance with Article 47 of the Law on Health Documentation and Records in the Field of Healthcare, access to the patient's e-record, i.e. medical documentation, is granted to the chosen doctor or a specialist physician. It was also stated that employees access the information system by means of a username and password known only to the employee, and that an amendment to the Rulebook on Information System Security is planned, bearing in mind that a new software solution has been introduced. Due to the well-founded suspicion that the Controller committed a misdemeanour under Article 95(1) of the LPDP, the Commissioner submitted a Request for the initiation of misdemeanour proceedings to the competent court.

Case Number: 072-21-3220/2025-07

1.15. Disclosure by Transmission of Health Data

From the operative part:

The specialist medical practice, as the Controller, is WARNED because, by disclosing through transmission the personal data contained in the "Service Users' Logbook", which includes health data and other data, namely: serial number, date on which the service was provided, name and surname, year of birth, street and number, UMCN, diagnosis, description of the procedure (what was performed), follow-up, price, facsimile and signature of the doctor, it delivered these data to the patient, as well as the data relating to nine other natural persons (patients), thereby violating the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the Law on Personal Data Protection, as well as the principle of "integrity and confidentiality" under Article 5(1)(6) of the same Law.

Part of the established factual situation:

The complainant stated that the Controller had sent her, via the Viber application, a message containing a photograph clearly displaying personal data of a patient, including health data and other details, relating to nine additional individuals (patients), namely: serial number, date on which the service was provided, name and surname, year of birth, street and number, unique citizen identification number, diagnosis, description of procedure (what was performed), follow-up, price, facsimile and the doctor's signature.

The Controller's representatives declared the following: the allegations from the complaint are accurate, and such conduct occurred with the intention of reassuring the complainant that her entry had been duly recorded in the protocol; the photograph in question was intended solely for her; everything happened "in haste" in order to respond as quickly as possible, during which they failed to anonymise the data of other service users/patients. The list in question, the "Service Users' Protocol", contains personal data of service users such as: serial number, date on which the service was provided, name and surname, year of birth, street and number, unique citizen identification number, diagnosis, description of procedure (what was performed), follow-up, price, facsimile and the doctor's signature. The list contains a total of ten (10) individuals, including the complainant. The message via the Viber application was sent by the clinic's owner and legal representative. The personal data of each patient are collected and processed in accordance with the Law on Health Care and the Law on Health Documentation and Records in the Field of Health. The data in question were not further disclosed, i.e. the records in question are not sent to anyone, and the incident occurred only in this particular case when the complainant was sent data relating to other service users. Only employees (doctors) and

the administrative staff member have access to the "Service Users' Protocol", which exists solely in hard-copy form and is kept in a locked cabinet.

Based on the established facts and the evidence collected, the Controller is hereby advised, with respect to the application of the LPDP, of the following.

Item 3) of Article 4 of the LPDP prescribes that the term "processing of personal data" shall mean any operation or set of operations performed, whether automated or non-automated, on personal data or on sets of personal data, such as collection, recording, sorting, grouping or structuring, storage, adaptation or alteration, disclosure, access, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, comparison, restriction, erasure or destruction.

Item 16) of Article 4 of the LPDP prescribes that "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person's health status.

Article 5, paragraph 1, items 1) to 6) of the LPDP prescribe the principles of personal data processing.

Article 12, paragraph 1 of the LPDP prescribes that the processing of personal data shall be lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically determined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject or for taking steps, at the request of the data subject, prior to entering into a contract; 3) the processing is necessary for compliance with the Controller's legal obligations; 4) the processing is necessary for the protection of the vital interests of the data subject or of another natural person; 5) the processing is necessary for the performance of tasks carried out in the public interest or in the exercise of statutory powers vested in the Controller; 6) the processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a minor.

Article 17 of the LPDP regulates the processing of special categories of personal data. Paragraph 1 of that Article prescribes that processing revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, is prohibited. Paragraph 2, items 1) to 10) of the same Article prescribe the circumstances in which the processing referred to in paragraph 1 of that Article is exceptionally permitted.

Article 42, paragraph 1 of the LPDP prescribes that, taking into account the level of technological development and the costs of its implementation,

the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons arising from the processing, the Controller, when determining the manner of processing and during the processing itself, is obliged to: 1) apply appropriate technical, organisational and personnel measures, such as pseudonymisation, which are aimed at ensuring the effective application of the principles of personal data protection, such as the reduction of the volume of data; 2) ensure the application of the necessary protection mechanisms during the processing, in order to meet the conditions for processing prescribed by this Law and to protect the rights and freedoms of the data subjects.

Paragraph 2 of the same Article of the LPDP prescribes that the Controller is obliged, through the continuous application of appropriate technical, organisational and personnel measures, to ensure that only those personal data which are necessary for achieving each individual processing purpose are always processed, and that this obligation applies to the number of data collected, the scope of their processing, the period of their storage and their accessibility.

Article 50 of the LPDP prescribes, inter alia, that, in line with the level of technological development and the costs of its implementation, the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical, organisational and personnel measures in order to achieve an adequate level of security relative to the risk.

The Health Care Act ("Official Gazette of the RS", Nos. 25/2019, 92/2023 – authentic interpretation, and 29/2025 – Constitutional Court decision) regulates the health care system in the Republic of Serbia, its organisation, the social care for the health of the population, matters of public interest in health care, oversight of the implementation of this Act, as well as other issues relevant to the organisation and provision of health care.

The Health Documentation and Records in the Field of Health Care Act ("Official Gazette of the RS", No. 92/2023) regulates health documentation and records in the field of health care, the types and content of health documentation and records, the manner and procedure for keeping them, the persons authorised to maintain health documentation and enter data, data processing, the manner of handling data from patients' medical documentation used for data processing, ensuring the quality, protection and preservation of data, as well as other matters of relevance for the establishment, organisation, maintenance and development of the integrated health information system – the Republic Integrated Health Information System. This Act, in Article 7, prescribes that personal data contained in medical and health documentation shall be processed in accordance with this Act, other laws governing personal data processing, and the law regulating per-

sonal data protection. Article 38 of the same Act prescribes that data from a patient's medical documentation constitute a special category of personal data and that health care institutions, private practices and other legal entities are obliged to collect and process personal data of patients in a manner that ensures the exercise of the right to privacy and the right to confidentiality of the patient's personal data, in accordance with the law governing patients' rights and the law governing personal data protection. Article 52 of the same Act provides that the processing of personal data contained in health documentation and records shall be carried out in accordance with the law regulating personal data protection (paragraph 1). The same Article, paragraph 2, prescribes that health care institutions, private practices and other legal entities, the Ministry of Defence, as well as authorised health professionals, health associates and other authorised persons who maintain medical documentation and records in accordance with this Act and the regulations adopted for its implementation, are obliged to protect medical documentation and patient records from unauthorised access, viewing, copying and misuse, irrespective of the form in which the data from the medical documentation are stored.

Having regard to the foregoing, it was established in the course of the subject inspection oversight procedure that the Controller, via the "Viber" application, in the process of enabling a patient to exercise the right of access to his or her personal data, forwarded to the patient a message containing a photograph clearly displaying the personal data of nine other patients (natural persons). These data included health data alongside other information, namely: serial number, date on which the service was provided, name and surname, year of birth, street and number, unique personal identification number (JMBG), diagnosis, description of the procedure (what was performed), follow-up, price, the physician's facsimile and signature. By acting in this manner, without a lawful basis, the Controller infringed the principle of "lawfulness, fairness and transparency" and the principle of "integrity and confidentiality"

Case Number: 072-04-3319/2025-07

1.16. Making an employee's health data available to the employer without a legal basis

From the operative part:

A WARNING is issued to the Controller because decision no. … of …, which contains data on the health condition of A.A. and other personal data from the complainant's medical documentation (diagnoses, description and timing of medical interventions, information on family medical history), was made available to a third party, thereby breaching the provisions

of Article 5(1)(1) and (6), Article 42(1)(2), and Article 50(2)(4) of the Law on Personal Data Protection.

Part of the established factual situation:

The Controller forwarded the second-instance decision, which contains detailed excerpts from the findings, opinion and assessment of the Second-Instance Medical Expert Body regarding the complainant's state of health and the data from her medical documentation to her employer.

Article 12(1) of the Law on Personal Data Protection prescribes that the processing of personal data is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of their personal data for one or more specifically defined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject or for taking steps, at the request of the data subject, prior to entering into a contract; 3) the processing is necessary for compliance with the Controller's legal obligations; 4) the processing is necessary to protect the vital interests of the data subject or another natural person; 5) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; 6) the processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, especially where the data subject is a minor.

The processing of special categories of personal data is regulated by Article 17 of the Law on Personal Data Protection. Paragraph 1 of that Article prescribes that processing revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, *data concerning health status*, or data concerning a person's sex life or sexual orientation, is prohibited, *while the exceptions under which such processing is permitted are set out in Paragraph 2 of the same Article*.

Article 42(1)(2) of the Law on Personal Data Protection prescribes that, taking into account the level of technological development and the costs of its implementation, the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risks to the rights and freedoms of natural persons arising from the processing, the Controller is obliged, when determining the manner of processing and during the processing itself, to ensure the application of the necessary protective mechanisms during the processing, so as to meet the conditions for processing prescribed by this Law and to safeguard the rights and freedoms of the data subjects. Paragraph 2 of the same Article prescribes that the Controller must, through the continuous application of appropriate technical, organisational and staffing measures, ensure that only those personal data

which are necessary for achieving each individual purpose of the processing are processed at all times, and that this obligation applies to the number of personal data collected, the scope of their processing, the period of their storage, and their accessibility.

Article 50(1) and (2) of the Law on Personal Data Protection, inter alia, provides that, taking into account the level of technological development and the costs of its implementation, the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risks to the rights and freedoms of natural persons, the Controller shall implement appropriate technical, organisational and staffing measures in order to achieve an adequate level of security in relation to the risk, and that, where necessary, such measures shall particularly include, inter alia, regular testing, assessment and evaluation of the effectiveness of technical, organisational and staffing measures for ensuring the security of processing. Paragraph 3 of this Article prescribes that, when assessing the appropriate level of security referred to in Paragraph 1, particular account shall be taken of the risks of processing, especially the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Based on the facts established in the course of the inspection supervision procedure, it was determined that the Controller, without any legal basis, and therefore in contravention of the principle of lawfulness, fairness and transparency of processing under Article 5(1)(1) of the Law on Personal Data Protection, which requires that data be processed *lawfully*, fairly and transparently in relation to the data subject, *and that processing is lawful only if carried out in accordance with this Law or another law governing processing*, made available to a third party the complainant's data concerning her state of health by delivering the second-instance decision containing detailed quotations of the findings, opinion and assessment of the Second-Instance Medical Assessment Body, as well as data from the complainant's medical documentation.

In addition, it was established that Article 5(1)(6) of the Law on Personal Data Protection, that is, *the principle of integrity and confidentiality*, was violated, as well as Articles 42(1)(2) and 50(2)(4) of the same Law, because the Controller, who is obliged under the Law on Personal Data Protection to process personal data by taking all necessary technical, organisational and staffing measures and to conduct regular testing, assessment and evaluation of the effectiveness of technical, organisational and staffing measures in order to protect the personal data it processes from destruction, alteration, unauthorised disclosure and unauthorised access, failed to identify deficiencies in their implementation. The Controller did not take sufficient or appropriate organisational and staffing measures prior to the personal data breach—measures which could and should have reduced the

risk of such or similar breaches to the lowest possible level. It is particularly relevant that, in this case, the Controller processes special categories of personal data and that its processing activities concern a large number of individuals. The Controller was obliged to act preventively, that is, to take appropriate organisational and staffing measures to prevent such conduct from occurring, especially bearing in mind that the internal act regulating the Controller's procedure in second-instance proceedings does not regulate the method of delivering decisions, which resulted in the absence of detailed guidance concerning the duties and responsibilities of employees in the processing of personal data

Action taken by the Controller:

The Controller notified the Commissioner that, after becoming aware of the breach of the provisions of the Law on Personal Data Protection, it had undertaken an extraordinary review of the decisions issued by employee B.B. from the date on which she was assigned to duties in second-instance proceedings, and that a further notice had been sent to all employees reminding them of their obligation to comply with the established procedures and the provisions of the Law on Personal Data Protection. It was also stated that, in order to prevent a recurrence of similar omissions, the Controller had amended its internal act to specify to whom the second-instance decision on appeal is to be delivered, and that it plans to introduce a personal data protection segment in all training seminars, regardless of the primary training topic, as well as to issue more frequent email notices reminding employees of their obligations under the Law on Personal Data Protection, including the adoption of new instructions for conduct in recurring characteristic situations.

Case Number: 072-21-2277/2025-07

1.17. The complainant (the patient) states that his medical documentation was handled unlawfully and that his rights as a patient were violated, as Health Centre X, without his consent, provided his medical record to Occupational Medicine Institute Y, to which the same patient had been referred.

According to the Commissioner's opinion:

The fundamental principles of personal data processing are prescribed by Article 5(1) of the Law on Personal Data Protection, under which personal data must: 1) *be processed lawfully*, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"). *Lawful processing is processing carried out in accordance with this Law or another law governing processing*; 2) be collected *for purposes that are specific, ex-*

plicit, justified and lawful, and must not be further processed in a manner incompatible with those purposes ("purpose limitation"); 3) be adequate, relevant and limited to what is necessary in relation to the purposes of the processing ("data minimisation"); 4) be accurate and, where necessary, kept up to date. Taking into account the purpose of processing, all reasonable steps must be taken to ensure that inaccurate personal data are erased or rectified without delay ("accuracy"); 5) be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed ("storage limitation"); 6) be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by implementing appropriate technical, organisational and personnel measures ("integrity and confidentiality").

Paragraph 2 of the same Article stipulates that the controller is responsible for compliance with the provisions of paragraph 1 and must be able to demonstrate such compliance ("accountability").

Pursuant to Article 12(1) of the Law on Personal Data Protection, *processing is lawful only if one of the following conditions is met*:

1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes;
2) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps, at the request of the data subject, prior to entering into a contract;
3) the processing is necessary *for compliance with the controller's legal obligations*;
4) the processing is necessary in order to protect the vital interests of the data subject or another natural person;
5) the processing is necessary for the performance of a task carried out in the public interest or *in the exercise of official authority vested in the controller*;
6) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a minor.

Paragraph 2 of the same Article stipulates that point (6) of paragraph 1 does not apply to processing carried out by a public authority within the scope of its competences.

In line with the foregoing, the data subject's consent is not the sole legal basis for the processing of personal data.

Article 17 of the Law on Personal Data Protection regulates the processing of so-called special categories of personal data. Paragraph 1 of that Article provides that processing revealing racial or ethnic origin, political

opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, is prohibited. Points 1) to 10) of paragraph 2 of the same Article set out the cases in which *the processing referred to in paragraph 1 is, exceptionally, permitted*. Among other things, point 8) stipulates that processing is permitted where it is necessary for the purposes of *preventive or occupational medicine, the assessment of an employee's working capacity*, medical diagnosis, the provision of health or social care, or *the management of health* or social-care *systems, on the basis of a law* or a contract with a health-care professional, provided that the processing is carried out by, or under the supervision of, a health-care professional or another person who is subject to an obligation of professional confidentiality prescribed by law or professional rules.

Article 21 paragraphs 1, 2 and 4 of the Law on Patients' Rights ("Official Gazette of the RS", Nos. 45/2013 and 25/2019 – amended by law) prescribe that data concerning a person's state of health, i.e. data contained in medical documentation, constitute personal data and represent particularly sensitive personal data of the patient, in accordance with the law (paragraph 1); that the data referred to in paragraph 1 of this Article must be kept confidential by all health-care professionals and health associates, as well as other persons employed in health-care institutions, private practices, organisational units of higher-education institutions of health-care professions which perform health activities, other legal persons performing certain health-care activities in accordance with the law, the compulsory health-insurance organisation, as well as the legal person providing voluntary health insurance with which the patient is insured, *where such data are accessible and necessary for the exercise of their statutory competences* (paragraph 2); and that the persons referred to in paragraph 2 of this Article, as well as any other persons *who, without authorisation* or without the consent of the patient or their legal representative, handle data from the medical documentation contrary to this Article *and disclose such data to the public without authorisation*, shall be responsible for the unauthorised disclosure of particularly sensitive data, in accordance with the law.

Article 22 of the same Law prescribes that the duty to maintain the confidentiality of the data referred to in Article 21 paragraph 1 of this Law, vested in the competent health-care professionals or health associates, as well as other persons employed by the employers referred to in Article 21 paragraph 2 of this Law, may be waived only on the basis of the patient's written consent, or the written consent of their legal representative, or on the basis of a court decision (paragraph 1); where the patient, or the legal representative, has given written consent or an authorisation certified by the competent authority, which is kept in the medical documentation, for

the communication of data on the state of health, the competent health-care professional may communicate the patient's health data; and that, by way of exception to paragraph 2 of this Article, the competent health-care professional may communicate data on the patient's state of health to an adult member of the immediate family even where the patient has not given consent for the communication of their health data, if such communication is necessary in order to avoid a health risk to that family member.

In accordance with the foregoing, and bearing in mind that the patient was referred for an examination and assessment of working ability to the Institute, the patient's position that there was an "unlawful handling" of his medical documentation is incorrect and without legal basis, as is the view that consent was required as the legal basis for the processing of his personal data by both health-care institutions. This is because the Institute requires his medical documentation from the aforementioned Health Centre in order to exercise its statutory competences.

Case Number: 072-21-4747/2025-07

1.18. The controller used a video-surveillance system for the purpose of monitoring and recording an employee's attendance at work, and as evidence in disciplinary proceedings.

From the operative part:

The Commissioner issued a warning to the Controller because the Controller used the employee's personal data, collected through the video-surveillance system, for the purpose of monitoring and recording the employee's attendance at work and as evidence in disciplinary proceedings, thereby breaching Article 5(1)(1) of the Law on Personal Data Protection, namely the principle of lawfulness, fairness and transparency, as the employee's personal data were not processed in accordance with the LPDP or any other law governing the processing of personal data; and Article 5(1)(2) of the LPDP, namely the principle of purpose limitation, as the employee's personal data were not collected for purposes that were specifically defined, explicit, justified and lawful, and were further processed in a manner incompatible with those purposes.

From the reasoning:

During the supervisory procedure, it was established that the Controller had used footage collected through the installed video-surveillance system as evidence in disciplinary proceedings conducted against an employee. Given that no other law governing the field of labour and employment (the Labour Law

and the Law on Records in the Field of Labour) prescribes that employee attendance at work may be monitored or recorded by means of a video-surveillance system, and that such processing is not carried out in accordance with the relevant provisions of the Law on Private Security, the Controller breached the principle of lawfulness, fairness and transparency under Article 5(1)(1) of the LPDP, as there was no legal basis for the processing described.

By using the video-surveillance system for the purpose of monitoring employees' attendance at work and, consequently, for establishing a breach of work discipline by an employee, the Controller acted contrary to the principle of purpose limitation under Article 5(1)(2) of the LPDP, as the personal data in this case were not collected for purposes that were specifically defined, explicit, justified and lawful, and were further processed in a manner incompatible with those purposes.

Action taken by the Controller:

On the basis of the corrective measure imposed, the Controller stated, by letter No. 32/10-4377-1875 of 12 November 2025, that the "relevant data" were no longer subject to processing, given that the retention period had expired, as a result of which their further processing had been restricted.

The Controller also stated that, in order to prevent similar situations from recurring, the following measures had been envisaged: establishing an internal log of access to video-surveillance recordings for the purpose of recording and monitoring any potential unauthorised processing of data; conducting regular compliance checks with personal data protection regulations, to be carried out by the Data Protection Officer at least once a year; ensuring that video-surveillance recordings are not used, either by the Controller or by other persons, for purposes that are not in accordance with the law and with the Decision on the Introduction of Video Surveillance. Due to reasonable suspicion that the Controller committed a misdemeanour under Article 95(1)(1) of the LPDP, the Commissioner submitted a Request for the Initiation of Misdemeanour Proceedings to the competent court.

Case Number: 072-04-3201/2025-07

1.19. Processing of Personal Data through a Video-Surveillance System in Public Bus Passenger Transport

From the operative part:

The Controller is issued a warning because:

1) it instructed the transport operators with whom it had concluded public–private partnership contracts for the provision of the municipal service of public urban, local and suburban bus passenger

transport to inform passengers of the existence of video surveillance in the vehicle and of the recording of the passenger area, by marking the vehicles with stickers whose content was determined by the Controller, and which do not contain all the information required under Article 23 of the Law on Personal Data Protection, thereby acting contrary to the principle of "*lawfulness, fairness and transparency*" under Article 5(1)(1) of the Law on Personal Data Protection;

2) before commencing the processing of data within the video-surveillance system, it failed to regulate the processing with the transport operators with whom it had concluded public–private partnership contracts for the provision of the municipal service of public urban, local and suburban bus passenger transport, in their capacity as processors, by means of a contract or other legally binding act concluded in written form, in accordance with the cited statutory provision, thereby acting contrary to Article 45(3) of the Law on Personal Data Protection.

Part of the established factual situation:

Based on the facts established in the course of the inspection supervision procedure, it was determined that the Controller violated the provisions of the Law on Personal Data Protection, as stated in the dispositive of this act. Namely, during the supervision it was established that the Controller had sent to the transport operators with whom contracts on public–private partnerships for the performance of the municipal service of public urban, local and suburban bus passenger transport had been concluded, a notice … dated … regarding their obligation to inform passengers of the existence of video surveillance in the vehicle and of the recording of the passenger area, by marking the vehicles with stickers whose content had been determined by the Controller, whereby only a video-surveillance pictogram was used to inform passengers, disregarding the obligation to provide all other information required under Article 23 of the Law on Personal Data Protection. At the moment of collecting personal data, the Controller did not provide users of public bus transport services with all relevant information concerning the processing of personal data prescribed by the cited provision of the Law on Personal Data Protection, thereby acting contrary to the principle of *lawfulness*, fairness and transparency of processing under Article 5(1)(1) of the Law, which requires that data be processed lawfully, fairly and transparently in relation to the data subject.

Furthermore, it was established that the Controller violated Article 45(3) of the Law on Personal Data Protection, because, prior to commencing the processing of data within the video-surveillance system, the Controller did not regulate the processing with the transport operators with whom public–private partnership contracts for the performance of the

municipal service of public urban, local and suburban bus passenger transport had been concluded, in their capacity as processors, by means of a contract or other legally binding act concluded in written form, including electronic form, which binds the processor to the controller and sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, as well as the rights and obligations of the Controller.

Action taken by the Controller:

The Controller submitted a letter to the Commissioner informing the Commissioner that the Controller had provided all transport operators with a new design of the sticker relating to the processing of personal data by means of video surveillance and that the placement of the stickers was in progress; that an "Information Notice on the Processing of Personal Data through the Video Surveillance System in Public Passenger Transport Vehicles" had been published on the Controller's website; and that standard contractual clauses had been prepared which will be concluded with all transport operators under the public–private partnership agreements.

Case Number: 072-04-3532/2024-07

1.20. By its decision, the secondary school X, as the Controller, was prohibited from processing the personal data of employees and pupils through the video-surveillance system installed in two classrooms – the ICT classroom and the tailoring workshop; it was ordered to erase all personal data, that is, all recordings generated by that video-surveillance system, and to inform the employees and pupils whose recordings had been stored from the moment of installation until the moment the video-surveillance system was switched off.

From the operative part:

The Controller violated the provisions of Article 5(1)(1), (2) and (3) of the LPDP, as it processed personal data contrary to the principles of "lawfulness, fairness and transparency", the principle of "purpose limitation", and the principle of "data minimisation".

From the reasoning:

The Commissioner, through an authorised person and in accordance with Article 78(2) of the LPDP, carried out an extraordinary on-site inspection of the Controller's compliance with the LPDP, based on information obtained from the complaint, which raised concerns that the processing of

personal data through the installed video-surveillance system was being carried out contrary to the provisions of the LPDP.

The facts established as decisive in the course of the inspection, on the basis of statements given by the Controller's representatives, a review of the available documentation, and an on-site inspection of the premises and equipment, are as follows:

- The immediate reason given for installing video surveillance in the tailoring classroom was the damage caused to a professional iron, for which no one accepted responsibility (that is, the teachers supervising the pupils using the iron), as well as certain malfunctions of machines in the tailoring classroom for which the responsible person could not be identified. In the IT classroom, teachers had complained about the condition of the computers, specifically that applications downloaded from the Internet and not required for lessons had been installed, which placed an additional burden on the operation of the computers, despite the existence of a logbook in which the date, time and user of the classroom are recorded;
- The Controller had not adopted a decision on the introduction of video surveillance.
- No written notice was provided to teachers or pupils regarding the intention to introduce video surveillance.
- The cameras were installed in the following positions: in the IT classroom, one camera was positioned so *as to record the teacher's desk* and *all pupil workstations where they are seated while in the room*, while a second camera was installed at the corner of the wall above the door of the adjoining room within the same classroom, *capturing the teacher's desk and pupils seated at other workstations*. In the tailoring classroom, one camera was mounted on a beam located in the middle of the ceiling of the first section of the classroom, recording nine sewing machines and the pupils and teachers present; the second camera was installed in the second section of the classroom at the corner of the wall near the window, recording the other nine sewing machines and the tailoring table located in front of the iron. *The iron itself was not recorded, i.e. it was not visible.*
- A review of the real-time video feed on the monitor established that the stated classrooms were being recorded from all previously mentioned camera positions—*except for the iron, which, according to the Controller's representatives, was the item allegedly damaged and the stated reason for installing video surveillance*.

The principles of personal data processing set out in Article 5(1)(1), (2) and (3) of the LPDP prescribe that personal data must: 1) be processed lawfully, fairly and transparently in relation to the data subject ("lawfulness, fairness and transparency"). Lawful processing is processing carried

out in accordance with this Law or another law regulating the specific processing; 2) be collected for purposes that are specific, explicit, justified and lawful, and shall not be further processed in a manner incompatible with those purposes ("purpose limitation"); and 3) be adequate, relevant and limited to what is necessary in relation to the purpose of processing ("data minimisation").

Accordingly, processing is lawful only if it is carried out in accordance with the LPDP *or another law* regulating the specific data processing. Furthermore, for the processing of personal data to be lawful, in addition to having a legal basis, there must be *a specific, justified and lawful purpose*, and only data that are *adequate, relevant and limited to what is necessary to achieve the intended purpose* may be processed.

The processing of personal data in the field of education is regulated by the provisions of the Law on the Fundamentals of the Education System ("Official Gazette of the RS", Nos. 88/2017, 27/2018 – amended law, 10/2019, 27/2018 – amended law, 6/2020, 129/2021 and 92/2023) and, specifically, by the laws governing primary and secondary education. However, these laws do not regulate the processing of personal data by means of video surveillance.

Given that video surveillance is not regulated by the LPDP, and that recording by a video-surveillance system itself *constitutes a personal data processing operation* within the meaning of Article 4(3) of that Law, such processing is subject to the general principles laid down in Article 5(1) of the LPDP, as well as the relevant provisions of the Law on Private Security ("Official Gazette of the RS", Nos. 104/2013, 42/2015 and 87/2018).

The Law on Private Security ("Official Gazette of the RS", Nos. 104/2013, 42/2015 and 87/2018) regulates matters relating to video surveillance, the mandatory security and protection of certain facilities, the activities and work of legal and natural persons in the field of private security, the conditions for their licensing, the manner of performing such activities, and the supervision of their operations.

Article 31(2) of that Law stipulates that technical means used in the performance of private security activities *must not be used in a manner that infringes the privacy of others.*

Article 91(1) of the LPDP prescribes that, *in the field of labour* and employment, the provisions of the laws governing labour and employment and collective agreements shall apply, together with the application of the provisions of this Law. Paragraph 2 of the same Article prescribes that if the law governing labour and employment or a collective agreement contains provisions on personal data protection, special *measures must also be prescribed to safeguard the dignity of the individual*, the legitimate interests and the fundamental rights of the data subject, particularly with regard to the transparency of processing, the exchange of personal data within a

multinational company or a group of undertakings, as well as systems of monitoring in the workplace.

Pursuant to Article 30(1) of the Labour Law ("Official Gazette of the RS", Nos. 24/2005 … 95/2018), an employment relationship is established by an employment contract, while Article 34(1) of the same Law prescribes that an employee exercises rights and duties arising from the employment relationship *on the day they commence work.*

By commencing work and entering the work premises, the privacy of every individual in the capacity of an employee is reduced to some extent, compared with the degree of privacy the same individual enjoys outside the workplace. However, by entering the so-called work premises*, an employee is not completely deprived of their privacy*. Every employee has a right to a certain degree of privacy that they may reasonably expect at their workplace, both in relation to the employer and in relation to the broader environment in which they perform their work duties. The degree of privacy of an employee, in the part not regulated by law, is established and assessed on the basis of the above-mentioned data-processing principles contained in Article 5(1) of the LPDP, taking into account the nature of the work performed by the employee within the employer's business activity.

The Controller was advised that, in practice, cameras are installed at locations from which access is gained to the premises intended for the performance of regular business activities of the employer (such as corridors), while also taking into account the angle at which cameras cover a particular area, so as to avoid excessive processing of personal data. If an employer has high-risk work processes (involving health and safety risks, handling money, dangerous machines, hazardous materials, etc.), as well as premises with restricted access and specific protection measures (server rooms, laboratories, etc.), then it is justified to use video surveillance—and, where necessary, additional security measures (electronic code locks, magnetic access cards, etc.)—to monitor work processes and control access to such premises.

However, the nature of the work performed by the employees of the Controller, as well as the handling by pupils of equipment required for practical instruction in the relevant classrooms (laboratories), and the educational activity carried out by the Controller, do not require a security measure for the protection of property and operations that would justify such an invasive impact on the privacy of employees and pupils. The same purpose may be achieved through the use of fewer personal data and in a manner that is less intrusive to the privacy and other rights and freedoms of natural persons.

Article 5(2) of the LPDP prescribes that the Controller is responsible for the application of the principles set out in paragraph 1 of that Article.

One of those principles is the principle of "*data minimisation*" under Article 5(1)(3), which means that only those data may be processed that are *adequate, relevant and limited* to what is *necessary* in relation to the purpose of the pro-

cessing. This means that, in each specific case, it must be assessed whether the processing of particular data is *necessary and appropriate* for the **given purpose**, or whether the purpose may be achieved by processing some other data.

The fact established during the supervision is that the stated reason (purpose) for introducing video surveillance was damage to an iron in the tailoring classroom. However, an on-site inspection established that the area where the iron is located *is not within the camera coverage* in that classroom, which indicates that personal data are being collected through video surveillance for a purpose (the protection of the School's property) that is clearly not specifically *defined, explicit or justified*, and is therefore contrary to Article 5(1)(2) of the LPDP.

Furthermore, the reason (purpose) stated for installing video-surveillance cameras in the IT classroom – namely that "there had been complaints from teachers regarding the condition of the computers, in the sense *that applications* downloaded from the Internet and not needed by pupils for teaching purposes had been installed on them, *which additionally burdened the functioning of the computers*" – does not indicate *the necessity* of processing data through video surveillance for the purpose of protecting the School's property. Applications allegedly downloaded by pupils from the Internet can easily be uninstalled, and such conduct by pupils can be prevented through supervision by the teacher present.

This demonstrates that the recording of teachers and pupils by means of video surveillance in the relevant classrooms is also contrary to *the principle of lawfulness*, *fairness and transparency* under Article 5(1)(1) of the LPDP. Namely, this principle, in addition to compliance with the regulations governing personal data processing, entails the application of the standard of fairness in processing. It means that the Controller must take into account *the circumstances of the processing and the interests of the persons* whose data are being processed by this processing activity, as well as *the expectations of those persons* regarding privacy in the given circumstances of processing, particularly the psychological pressure that such processing undoubtedly causes due to the continuous recording of the behaviour of employees and pupils, which undermines the necessary degree of their privacy.

It is emphasised that the foregoing does not affect the permissibility of the Controller's use of video-surveillance systems in areas such as corridors, in front of classroom entrances, and similar locations.

Taking into account all facts relevant for the decision in this supervision procedure, as well as the cited statutory provisions, it has been established that the Controller processes personal data of employees and pupils through video surveillance in classrooms No. 4 (IT classroom) and No. 7 (tailoring classroom) contrary to Article 5(1)(1), (2) and (3) of the LPDP.

Case Number: 072-21-2349/2024-07

1.21. Processing of employees' personal data through a video-surveillance system for the purpose of recording and monitoring working hours

From the operative part:

The Commissioner issued a warning to legal entity X, as the controller of personal data, because by processing personal data – namely by recording via a video-security device, i.e. a camera installed in the shift supervisor's office at the Controller's headquarters, capturing data relating to employees who are present in or move through that space during working hours – it violated the provisions of Article 5(1)(1) and (2) of the Law on Personal Data Protection, i.e. the principles of "lawfulness, fairness and transparency" and "purpose limitation".

From the reasoning:

In the course of the supervisory procedure, it was established, inter alia, that the Controller had introduced an electronic system for recording and monitoring working hours by means of IDM cards, for the purpose of determining the start and end of employees' working hours, the duration of breaks during working time, and absences from work during working hours; and that video surveillance had been introduced in order to prevent misuse of the electronic system for monitoring and recording working hours, as certain employees were misusing the system by having one employee swipe two or more IDM cards (i.e. their own card and the card of a colleague who was not present). It was established that the Inspected Entity had independently installed the video-surveillance system in question – a single camera in the shift supervisor's office, where the electronic system for recording and monitoring working hours by means of IDM cards is located; that the camera records in real time; and that it is directed towards the device used for recording working hours, for the purpose of monitoring the electronic system for recording and monitoring working hours.

Article 5(1)(1) of the Law on Personal Data Protection prescribes that personal data must be processed lawfully, fairly and transparently in relation to the data subject, and that lawful processing is processing carried out in accordance with this Law or another law governing processing ("lawfulness, fairness and transparency"). Article 5(1)(2) prescribes that personal data must be collected for purposes that are specifically defined, explicit, justified and lawful, and must not be further processed in a manner that is incompatible with those purposes ("purpose limitation"). Article 5(2) prescribes that the controller is responsible for applying the provisions of paragraph 1 of this Article and must be able to demonstrate such compliance ("accountability").

Article 12(1) of the Law on Personal Data Protection prescribes that processing is lawful only if one of the following conditions is fulfilled:

1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject or in order to take steps, at the request of the data subject, prior to the conclusion of the contract; 3) the processing is necessary for compliance with the controller's legal obligations; 4) the processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) the processing is necessary for the performance of tasks carried out in the public interest or in the exercise of the controller's statutory powers; 6) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, especially where the data subject is a minor.

Article 91(1) of the Law on Personal Data Protection prescribes that the processing of personal data in the field of labour and employment is subject to the provisions of the laws governing labour and employment, and collective agreements, with the application of the provisions of this Law.

Article 12(1) of the Labour Law ("Official Gazette of the RS", Nos. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – Constitutional Court decision, 113/2017 and 95/2018 – authentic interpretation; hereinafter: the Labour Law) prescribes, inter alia, that an employee has the right to the protection of personal integrity and human dignity.

Article 2(1), points 1 and 4 of the Law on Records in the Field of Labour ("Official Gazette of the FRY", No. 46/96 and "Official Gazette of the RS", Nos. 101/2005 – other law and 36/2009 – other law; hereinafter: the Law on Records in the Field of Labour) prescribe that, in the field of labour, a record of employed persons and a record of employees' earnings shall be established. Article 5(1), point 13 of the Law on Records in the Field of Labour prescribes that the record of employed persons contains data on working hours – expressed in hours (weekly). Article 23 of the same Law prescribes that the record of employees' earnings shall contain data on working hours, gross earnings, net earnings, net wage compensation, gross wage compensation financed by the employer, supplements, allowances and other payments, as well as gross earnings realised from other employers, while Article 24 prescribes that the record of employees' earnings shall, inter alia, contain data on working hours and their utilisation.

The processing of personal data through video surveillance and other technical means is regulated by the Law on Private Security ("Official Gazette of the RS", Nos. 104/2013, 42/2015 and 87/2018; hereinafter: the Law on Private Security), while the manner of performing technical protection activities and the use of technical means in the performance of private security activities, including video surveillance, is further regulated by the

Rulebook on the Manner of Performing Technical Protection Activities and the Use of Technical Means ("Official Gazette of the RS", No. 91/2019).

Technical protection is the protection of persons and property carried out by means of technical equipment and devices, including their planning, design, installation and maintenance, as prescribed by Article 3(1), point 22 of the Law on Private Security.

Article 29 of the Law on Private Security prescribes that technical protection activities are performed through the use of technical equipment and devices to prevent unlawful acts against persons, property or business operations, particularly for protection against: 1) unauthorised access to protected premises and facilities; 2) removal, misappropriation or unauthorised use of protected items; 3) bringing weapons, explosive, radioactive or other hazardous objects and substances into protected premises; 4) burglary, sabotage and violent attack on a facility or the seizure of items; 5) unauthorised access to data and documentation; 6) protection of vehicles for the transport of money and other transport vehicles; 7) other identified risks.

Article 30(1) of the Law on Private Security prescribes, inter alia, that the use of technical means and devices for the protection of persons, property and business operations shall be understood to mean services provided through the application of individual or functionally connected perimeter measures, devices and systems for: intrusion and hold-up protection, fire protection, video surveillance, access control, social alarms, satellite vehicle tracking (GPS), electrochemical protection of valuables, mechanical protection and data protection.

Article 31 of the Law on Private Security prescribes that technical protection shall be carried out on the premises of a protected facility or area, during the protection of protected persons, property and business operations, or during the protection of the transport of money and valuable consignments, and that technical equipment used in the performance of private security activities must not be used in a manner that violates the privacy of others.

Based on the established facts that the Controller uses recordings from the video-surveillance camera for the purpose of overseeing the electronic system for monitoring and recording working hours, i.e. for the purpose of preventing misuse of the electronic system for monitoring and recording working hours, and taking into account the provisions of the Law on Personal Data Protection relating to the principles of "lawfulness, fairness and transparency" and "purpose limitation", the provisions of the Labour Law and the Law on Records in the Field of Labour concerning the Controller's statutory authorisation to process personal data on employees' working hours within the records kept in the field of labour, as well as the provisions of the Law on Private Security relating to the purpose and

manner of carrying out technical protection by means of video surveillance, the Controller, in the manner described, processes employees' personal data contrary to Article 5(1)(1) and (2) of the Law on Personal Data Protection, which prescribes that lawful processing is processing carried out in accordance with that Law or another law governing processing, and that personal data must be collected for specific, explicit, legitimate and justified purposes and must not be further processed in a way that is incompatible with those purposes.

The Controller is specifically emphasised that this does not deny its statutory authorisation to process data on employees' working hours within the records kept in the field of labour, and that, bearing in mind that no other law prescribes the processing of employees' personal data in the sense of accessing video-surveillance recordings for the purpose of monitoring the recording of working hours, the lawfulness of the processing at issue is assessed on the basis of the provisions of the Law on Personal Data Protection.

Case Number: 072-21-1549/2024-07

1.22. Processing of personal data of tenants of a residential community collected through a video-surveillance system

From the operative part:

The Commissioner issued a warning to Residential Community X, as the controller of personal data, because it was processing personal data through a video-surveillance system installed and maintained by a sole trader who did not hold a valid licence prescribed by the Private Security Act; and because it published, on the notice board in the entrance of the residential building, photographs of natural persons taken from the video-surveillance system and, without any legal basis, made them available to an indeterminate number of third parties, thereby acting contrary to the principle of "lawfulness, fairness and transparency" laid down in Article 5(1)(1) of the LPDP. By publishing those photographs of natural persons, collected through the video-surveillance system, the controller further processed the personal data in a manner incompatible with the purpose for which they had been collected, thereby acting contrary to the principle of "purpose limitation" laid down in Article 5(1)(2) of the same law. Furthermore, by enabling a number of tenants, via a mobile application and a TV receiver, to monitor in real time the footage from the surveillance cameras installed in the building's common areas—footage relating to tenants and other individuals who reside in or pass through those areas—the controller acted contrary to the principle of "data minimisation" laid down in Article 5(1)(3) of the same law.

From the reasoning:

In the course of the supervisory procedure it was established, inter alia, that the Controller had posted photographs of natural persons—namely one resident of the building and one unidentified person—on the notice board in the entrance of the residential building, having previously taken those photographs from the building's video-surveillance system; that the professional building manager had posted those photographs in order for the residents to potentially identify the perpetrators of thefts committed in the building; that access to the video-surveillance system, specifically real-time viewing of footage via a mobile-phone application, is available to the professional building manager and several residents of the building, while the remaining residents are able to view the real-time footage via a television receiver.

Article 5(1)(1) of the LPDP prescribes that personal data must be processed lawfully, fairly and transparently in relation to the data subject, and that lawful processing is processing carried out in accordance with that Act or another law governing processing ("lawfulness, fairness and transparency"). Article 5(1)(2) prescribes that personal data must be collected for purposes that are specific, explicit, justified and lawful, and may not be further processed in a manner incompatible with those purposes ("purpose limitation"). Article 5(1)(3) prescribes that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes of the processing ("data minimisation"). Article 5(2) prescribes that the controller is responsible for complying with the provisions of paragraph 1 of that Article and must be able to demonstrate such compliance ("accountability").

Article 12(1) of the LPDP prescribes that processing is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject, or for taking steps at the request of the data subject prior to the conclusion of the contract; 3) the processing is necessary for compliance with the controller's legal obligations; 4) the processing is necessary for the protection of the vital interests of the data subject or of another natural person; 5) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's statutory powers; 6) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data, particularly where the data subject is a minor.

The processing of personal data through video-security systems and other technical means is regulated by the Law on Private Security ("Official

Gazette of the RS", Nos. 104/2013, 42/2015 and 87/2018; hereinafter: the LPS), while the manner of performing private-security activities, including video-security, is further regulated by the Rulebook on the Manner of Performing Technical Protection Activities and Use of Technical Means ("Official Gazette of the RS", No. 91/2019).

Article 3(1)(22) of the LPS prescribes that technical protection is the protection of persons and property carried out by means of technical equipment and devices, including their planning, design, installation and maintenance.

Article 6(1) of the LPS prescribes, inter alia, that legal entities and entrepreneurs engaged in private security, under the conditions laid down by that Act, may hold a licence for performing activities such as: risk assessment in the protection of persons, property and operations; planning, design and supervision of the implementation of technical-protection systems; installation, commissioning and maintenance of technical-protection systems; and user training.

Article 8(1) of the LPS prescribes that private-security activities may be performed by legal entities, entrepreneurs and natural persons who hold a private-security licence issued by the Ministry of the Interior (hereinafter: the Ministry).

Article 20(3) of the LPS prescribes that a legal entity or entrepreneur who does not hold a licence may not be engaged to perform private-security activities.

Article 30(1) of the LPS prescribes, inter alia, that the use of technical means and devices for the protection of persons, property and operations shall be understood as the provision of services through the application of individual or functionally connected perimeter measures, devices and systems for: anti-burglary and anti-robbery protection, fire protection, *video-security*, access control, social alarms, satellite vehicle tracking (GPS), electrochemical protection of valuables, mechanical protection and data protection.

Article 31(2) of the LPS prescribes that the technical means used in the performance of private-security activities may not be used in a manner that infringes the privacy of others.

Article 68(1) of the LPS prescribes that data collected in the performance of private-security activities may be used solely for the purpose for which they were collected and may not be disclosed to third parties or made public, unless otherwise prescribed or agreed.

Having regard to the provisions of the LPDP concerning the principles of "lawfulness, fairness and transparency", as well as the provisions of the LPS concerning the purpose and manner of carrying out technical protection by means of video-security, the Controller, by processing personal data through a video-surveillance system installed and maintained by an entre-

preneur who does not hold a valid licence prescribed by the LPS, processes personal data contrary to that Act, and thereby contrary to Article 5(1)(1) of the LPDP, which prescribes that lawful processing is processing conducted in accordance with that law or another law governing the processing.

By publishing photographs of natural persons on the notice board of the Residential Community, previously collected through the video-surveillance system, the Controller, in the manner described, made the personal data of those persons available to an indeterminate number of third parties without any legal basis. In doing so, the Controller further processed personal data collected for specifically defined purposes in a manner incompatible with those purposes, thereby breaching the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP and the principle of "purpose limitation" under Article 5(1)(2) of that law.

Enabling tenants to monitor images from cameras in real time, via internal or public cable television or a mobile application, or other electronic communication means capable of transmitting such recordings either at the moment they are created or subsequently, allows a wide circle of users to intrude—without any genuine need or justification—into the privacy of citizens, i.e. other tenants and individuals visiting them. This is contrary to the principle of "data minimisation" under Article 5(1)(3) of the LPDP. In relation to the above, the Controller is advised that the integrity and confidentiality of personal data must be ensured, meaning that technical, organisational and personnel measures must be implemented so that the system used for video-surveillance and the recordings generated by that system are protected from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. This also implies that access to the recordings from the video-surveillance system, including real-time monitoring of camera feeds, must be available solely to those persons for whom such access is necessary in order to fulfil the purpose of the processing.

Case Number: 072-21-2453/2025-07

1.23. Processing of personal data by audio-recording outgoing calls

From the operative part:

The controller, a bank, is WARNED because it: by audio-recording outgoing calls made by the Contact Centre, processed personal data contrary to the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP, and in connection with Article 5(2) of the LPDP, thereby carrying out that processing without an appropriate legal basis under Article 12(1) of the LPDP; by audio-recording both incoming and outgoing calls of the Contact Centre, processed personal data contrary to Article

23(1)(3) of the LPDP, and thus also contrary to the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP and in connection with Article 5(2) of the LPDP, because it did not provide the data subjects with information on the purpose of the intended processing.

From the reasoning:

The Commissioner received a complaint concerning the processing of personal data by the Controller, relating to the recording of telephone conversations without clear and timely notification, as well as inconsistencies between the Controller's practice and the official Personal Data Processing Notice available on its website. The complainant stated that he had been contacted by the Controller's Contact Centre by telephone, that he had not been informed that the conversation was being recorded; and that, only at the end of the call and upon his inquiry, the Contact Centre employee confirmed that all calls were recorded, which contradicted the information contained in the Personal Data Processing Notice published online. The complaint further states that, in relation to the complainant's request for access to his personal data, the Controller claimed that the relevant calls had not been recorded.

During the supervision procedure and based on the Controller's written submission, it was established that: since this was an outgoing call, and given that the Controller's Contact Centre does not record outgoing calls, i.e. calls initiated by the Controller towards users, no recording of the conversations held with the user was made or is available; that, when asked by the user about the call recording, the Contact Centre employee who conducted the telephone conversations explained that telephone calls with the Contact Centre are generally subject to recording for the purpose of improving service quality; that this relates exclusively to incoming calls; that the possibility of a misunderstanding in communication or an operational error by the employee cannot be excluded, but the Controller emphasised that it does not record outgoing calls; that the Controller's Contact Centre records a portion of incoming calls on the basis of legitimate interest under Article 12(1)(6) of the LPDP, for the purpose of improving the quality of customer support; that the recordings are used solely for the internal training of Contact Centre agents with a view to enhancing communication and providing higher-quality customer service; that all users are automatically notified, before a call with the Contact Centre is connected, via a voice message that their call may be recorded and used to improve the quality of service; that the processing includes audio recordings of conversations and basic call information (date, time and the number from which the call was received); and that the information referred to in Article 23 of the LPDP is provided through the Personal Data Processing Notice available on the Controller's website.

Authorised officers of the Commissioner carried out an inspection of the database used for storing audio files of telephone conversations and established that, when randomly selecting three conversations conducted by an agent, where the calls had been initiated by the Controller (outgoing calls), users had not been informed that the conversation might be recorded.

By calling the Controller's Call Centre (incoming calls), the Commissioner's authorised officers established that, upon selecting the desired service option at the very beginning of the call, the user was informed via a voice message that the conversation may be recorded.

By inspecting the Personal Data Processing Notice published on the Controller's website on the date of the supervision, it was found that, under the section "Types of personal data processed – (B) Other types of data", the following, inter alia, was stated: "If you communicate with the Bank's Contact Centre by telephone, you should be aware that telephone conversations are recorded, of which we will notify you at the beginning of the telephone conversation before recording begins, so that you have the possibility to discontinue the call." By inspecting the document "Balancing Test of the Bank and the data subject contacting the Bank", it was established that the Controller had carried out an assessment of legitimate interest in relation to audio recording of calls when a person contacts the Controller via the Contact Centre (incoming calls), for the purpose of improving the work of the Controller's Contact Centre.

In this respect, Article 5(1) of the LPDP sets out the principles of personal data processing.

Article 12(1) of the LPDP prescribes that the processing of personal data is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject, or for taking steps at the request of the data subject prior to entering into a contract; 3) the processing is necessary for compliance with the Controller's legal obligations; 4) the processing is necessary for the protection of the vital interests of the data subject or of another natural person; 5) the processing is necessary for the performance of tasks carried out in the public interest or in the exercise of the Controller's statutory authority; 6) the processing is necessary for the purposes of the legitimate interests pursued by the Controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require personal data protection, particularly where the data subject is a minor.

Article 23(1)(3) of the LPDP prescribes that, where personal data are collected from the data subject, the Controller must, at the time of data collection, provide that person with information on the purpose of the intended processing and the legal basis for the processing.

In the course of the subject inspection procedure, it was established that the Controller had been carrying out audio-recording of outbound calls made by the Controller's Contact Centre, although the condition for lawful processing under Article 12(1)(6) of the LPDP had not been fulfilled. Namely, the Controller was unable to demonstrate to the Commissioner the application of this legal basis within the meaning of Article 5(2) of the LPDP, which requires that the Controller provide evidence that, prior to commencing the processing, it had assessed its necessity for the purpose of pursuing its legitimate interest, or that of a third party, which is not overridden by the interests or fundamental rights and freedoms of data subjects requiring data protection. Nor did the Controller demonstrate that any other condition for lawful processing under Article 12(1) of the LPDP had been fulfilled in respect of this processing. By doing so, the Controller acted contrary to the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP, in conjunction with Article 5(2) of the LPDP.

Furthermore, as the inspection procedure established that the Controller provides data subjects with the information referred to in Article 23 of the LPDP through the above-mentioned Information on Personal Data Processing document, and that this document does not specify whether the recording of telephone conversations with the Contact Centre applies to inbound or outbound calls, nor which calls may be recorded, nor the purpose for which such audio-recording is carried out, the Controller thereby violated the same provision of the LPDP. The Controller also violated the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP, in conjunction with Article 5(2) of the LPDP, as it failed to demonstrate the application of this principle.

Case Number: 072-21-2828/2024-07

1.24. A public enterprise responsible for parking fee collection disclosed the personal data of service users to another company for the purpose of collecting due and unpaid debts, without informing the users that the creditor had changed.

From the operative part:

The Commissioner warned the Controller because, by means of a Contract on Assignment of Claims for Consideration, the Controller transferred to another company the personal data of parking service users who had failed to pay the surcharge parking tickets issued to them. The transferred data included: the user's name and surname, unique citizen identification number, and residential address. The Controller did so without first inform-

ing the data subjects of the assignment, thereby breaching the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP.

From the reasoning:

In the course of the inspection oversight procedure, it was established that the Controller breached the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP, because the data previously obtained from the Ministry of Internal Affairs for the purpose of initiating enforcement proceedings based on issued but unpaid special parking tickets were transferred to another company. The transferred data included the debtor's name and surname, unique citizen identification number, and residential address. The Controller failed to provide the data subjects with the necessary information under Article 24 of the LPDP, required in order to ensure fair and transparent processing. Namely, the LPDP requires fair and transparent processing of personal data, which in this specific case includes the right of service users to be informed about how and why the Controller uses their data. Transparent processing entails that the Controller clearly informs users that their data are being collected, the type of data collected and the purpose of the processing, who will have access to the data and under which circumstances—presented in an easily accessible and understandable manner, using clear and simple language.

Action taken by the Controller:

Acting upon the Warning, the Controller submitted a notice to the Commissioner stating, inter alia, that it had ceased assigning outstanding receivables to another company and that, accordingly, there is no possibility of repeating the established breach of the provisions of the LPDP.

Case Number: 072-21-2445/2025-07

1.25. The Processor acted contrary to the legally binding act regulating its relationship with the Controller

From the operative part:

The insurance representation agency, acting as a processor, is WARNED in relation to the processing of personal data it performs on behalf of the Controller, because it violated the principle of "integrity and confidentiality" under Article 5(1)(6) of the LPDP, which requires that personal data be processed in a manner that ensures appropriate protection of personal data, including protection against unauthorised or unlawful processing, as well as against accidental loss, destruction or damage, by implementing appropriate technical, organisational and staffing measures, and in

connection with Article 45 of the LPDP. Namely, by publishing a video on the social network "Instagram", as well as on the linked social network "Facebook", for the purpose of promoting insurance and raising awareness of the benefits of insurance, the processor disclosed the personal data of the insurance policyholder and two insured persons (the policyholder's minor children). The disclosed data concerned the following personal data of those individuals: unique citizen identification number (JMBG), name and surname, home address, occupation, family relationship, date of birth, telephone number and signature, as contained in the Life Insurance Offer, thereby violating the above provisions of the LPDP.

From the reasoning:

The Commissioner received a complaint stating that an insurance representation agency had published on its "Instagram" profile a video "in which the confidential personal data of the Policyholder and his minor children are clearly visible, including their unique citizen identification number (JMBG), name, surname and home address, displayed on the policy concluded with the insurance service provider."

Following the complaint, and for the purpose of collecting information relevant to a potential extraordinary inspection oversight, the Commissioner first requested the insurance service provider, as the Controller, to comment on the allegations contained in the submitted complaint.

On that occasion, the Controller stated the following:

"Pursuant to Article 97 of the Law on Insurance ('Official Gazette of the RS', Nos. 139/2014 and 44/2021), an Insurance Agent performs representation activities in insurance, namely the activities of initiating, proposing or carrying out the activities of preparing and concluding insurance contracts in our name and for our account, on the basis of an insurance representation agreement. The relationship between our Company and the Agent is regulated by the Insurance Representation Agreement and by a Personal Data Processing Agreement in written form, in accordance with Article 45 paragraphs 3 and 4 of the LPDP, under which the Agent is the processor in relation to the Controller. Under the signed Personal Data Processing Agreement, Article 5 paragraph 1 sub-paragraphs 10 and 11, the Agent was obliged to keep as confidential and secret all personal data entrusted or made available to him in connection with the implementation of the main agreement, i.e. the insurance representation agreement, and was obliged not to disclose, make available or transfer personal data to any third party without the prior consent of the Controller, unless required to do so under the law."

In addition, the Controller stated that the processor had been instructed to remove from social media the video recording in which the personal

data had been published, that they had received confirmation that the video had been deleted, and that a written statement from the processor had been obtained explaining the reasons for its actions.

In this regard, authorised officers of the Commissioner carried out an extraordinary inspection oversight of the Controller and of the insurance representation agency, in its capacity as processor, with the subject of oversight being the disclosure of personal data on the processor's "Instagram" profile and other social networks, arising in connection with the performance of insurance representation activities.

With respect to the questions posed, representatives of both the Controller and the processor jointly provided the following response:

"The insurance representation agency is, in relation to the insurance company, in the sense of the LPDP, acting as a processor engaged to perform representation activities in insurance. In the sense of the LPDP, the Controller has concluded with the processor a Personal Data Processing Agreement. The implementation of the appropriate technical, organisational and personnel measures for the protection of personal data has been regulated between the Controller and the processor under Article 5 of the Personal Data Processing Agreement. The processor performs its activities in the field of insurance representation in accordance with the Insurance Representation Agreement and the Personal Data Processing Agreement. The processor operates 'Instagram' and 'Facebook' social media accounts, which it uses for the purpose of promoting and raising awareness of the importance and necessity of insurance, as well as to promote its own production. In the present case, the video in question was published on the 'Instagram' social network, but, as these networks and accounts are linked, it was simultaneously published on the 'Facebook' social network as well. The processor does not otherwise publish personal data on these social networks; however, in the present case, during the promotion and awareness-raising activity concerning the importance and necessity of insurance, personal data of three individuals (the father and two minor children) were inadvertently disclosed by means of the created video recording, although such data had been collected solely for the purpose of preparing and concluding an insurance contract, which ultimately was not concluded. The Controller became aware of the processor's actions only after being contacted by the authorised officer of the Commissioner, following which the processor was contacted, the recordings in question were deleted from both social networks, and the processor was additionally instructed regarding the permissible processing of personal data for the purposes of insurance representation."

In this regard, the Commissioner established that Article 4 of the Personal Data Processing Agreement between the Controller and the processor sets out the Controller's obligations. Under this Agreement, the Controller

is obliged to: provide the processor with valid templates of the privacy notice and the consent form for personal data processing; provide the processor, in a timely manner, with written instructions regarding the manner of processing personal data; take all necessary technical and organisational measures concerning the IT infrastructure in order to prevent a personal data breach; provide the processor, upon request, with its internal acts governing personal data processing; provide the processor with all assistance reasonably necessary for the processor to fulfil its obligations under this Agreement and the law; appoint a person responsible for personal data processing who is authorised to provide responses concerning processing performed under the Principal Contract.

Furthermore, Article 5 of the Agreement prescribes the obligations of the processor.

Having regard to the established facts and the specific circumstances of the case, the Commissioner issued a warning for the following reasons.

Point 8) of the same Article of the LPDP defines the "controller" as a natural or legal person, or a public authority, that alone or jointly with others determines the purpose and means of the processing and also provides that the law which determines the purpose and means of the processing may designate the controller or prescribe the conditions for its designation.

Point 9) of this Article of the LPDP defines the "processor" as a natural or legal person, or a public authority, which processes personal data on behalf of the controller.

The principles of personal data processing are prescribed by Article 5(1) of the LPDP.

Article 12 of the LPDP prescribes that processing is lawful only if one of the conditions set out in points 1) to 6) is fulfilled.

Furthermore, Article 45(1) of the LPDP prescribes that, if processing is carried out on behalf of the controller, the controller may designate as a processor only such a person or public authority that fully guarantees the application of appropriate technical, organisational and staffing measures, in a manner that ensures that the processing is carried out in accordance with the provisions of this law and that the rights of the data subjects are protected. Processing by the processor must be regulated by a contract or another legally binding act concluded, or adopted, in written form, including electronic form, which is binding upon the processor in relation to the controller and which regulates the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, as well as the rights and obligations of the controller (Article 45(3) of the LPDP). Paragraph 4 of the same Article prescribes that the contract or other legally binding act referred to in paragraph 3 of this Article must stipulate that the processor shall: 1) process personal data solely on the basis of the controller's written instructions,

including instructions relating to the transfer of personal data to other states or international organisations, unless the processor is required by law to process such data. In that case, the processor shall inform the controller of that legal obligation before commencing the processing, unless the law prohibits the provision of such information for reasons of protecting an important public interest; 2) ensure that any natural person authorised to process personal data is bound by a duty of confidentiality or is subject to a statutory obligation of confidentiality; 3) take all necessary measures in accordance with Article 50 of this law; 4) comply with the conditions for engaging another processor in accordance with paragraphs 2 and 7 of this Article; 5) taking into account the nature of the processing, assist the controller, through appropriate technical, organisational and staffing measures and to the extent possible, in fulfilling the controller's obligations regarding requests for the exercise of data subjects' rights under Chapter III of this law; 6) assist the controller in fulfilling its obligations under Article 50 and Articles 52 to 55 of this law, taking into account the nature of the processing and the information available to the processor; 7) after completion of the contracted processing activities, and in accordance with the controller's instructions, delete or return to the controller all personal data and delete all copies thereof, unless the law prescribes an obligation of data retention; 8) make available to the controller all information necessary to demonstrate compliance with the processor's obligations under this Article, as well as information that enables and supports the controller's audit, including inspections carried out by the controller or another auditor authorised by the controller.

Having regard to the above, it was established that the controller, by means of a legally binding act, obligated the processor to: apply appropriate technical, organisational and staffing measures in a manner that ensures that the processing is carried out in accordance with the provisions of the LPDP and that the rights of the data subjects are protected; refrain from disclosing, making available or transferring personal data to any third party without the prior consent of the controller, except where required to do so under the law; ensure that any natural person authorised to process personal data is bound by an obligation of confidentiality or is subject to a statutory confidentiality obligation; treat all personal data entrusted to it or made available to it in connection with the performance of the Principal Contract, as well as after the expiry of the Principal Contract, as confidential and secret; and not disclose, make available or transfer personal data to any third party without the prior consent of the controller, except where required to do so under the law.

In this regard, the Commissioner determined that the processor acted contrary to the Agreement by publishing a video on the social network "Instagram", as well as on the linked social network "Facebook", for the

purpose of promoting insurance and raising awareness of the usefulness of insurance, thereby disclosing the personal data of the policyholder and two insured persons (the policyholder's minor children). The disclosed data included the following personal data: unique master citizen number, full name, residential address, occupation, kinship, date of birth, telephone number and signature, as contained in the Life Insurance Offer. By doing so, the processor acted in breach of the principle of "integrity and confidentiality" set out in Article 5(1)(6) of the LPDP, in connection with Article 45 of the LPDP.

Case Number: 072-04-2306/2025-07

1.26. Disclosure of personal data contained in a current account statement

From the operative part:

The trade union organisation is WARNED because, by making available on its website the current account transaction statement, it disclosed the personal data contained in the transaction statement relating to the accounts of natural persons, thereby violating Article 5(1)(1) of the LPDP. Consequently, it carried out the processing of personal data without an appropriate legal basis under Article 12(1) of that law and contrary to Article 17(1) and (2), which regulate the processing of special categories of personal data, including data relating to trade union membership.

From the reasoning:

The Commissioner for Information of Public Importance and Personal Data Protection received a complaint concerning the unauthorised prior publication of personal data (the complainant's name and surname, current account numbers and purpose of payment) on the website, relating to the data of members of the trade union organisation.

In this regard, a request for a written statement was sent to the trade union organisation, as the Controller, to which it responded as follows:

"Given that, once the court proceedings were concluded, the trade union organisation, headed by the lawful leadership, regained access to its accounts, the leadership—in the interest of transparency of financial flows, which represents one of the fundamental principles of trade union organisation, bearing in mind that the trade union is financed from the membership fees of its members who have every right to know how their money is being spent—published the account statements of the trade union organisation for the previous seven years. At the moment of publication, the trade union organisation was not aware that these statements contained

data on payments made to the bank accounts of natural persons, as this is not customary for a trade union organisation, which, as a rule, does not make payments to the bank accounts of natural persons; on the contrary, it is financed from the membership fees of natural persons through payments made by the employer on the basis of administrative deductions from employees' salaries. Given that this concerned a period of as many as seven years, the trade union organisation, immediately upon realising that payments had been made to private bank accounts of natural persons, deleted all statements from its official website."

Following the Controller's written statement, an extraordinary on-site inspection was carried out.

During the inspection, the Record established the following.

For the purpose of transparent management of the financial flows of the supervised entity and informing the members of the trade union, the Controller published on its website the statements from its current account (which had been made available to it for the first time after seven years by the banks), relating to the operations of the previous management of the Controller. On the assumption that the statements in question should not contain data relating to natural persons (as the payments should concern the Controller's relations with legal persons), the supervised entity published them on its website without a detailed review of the individual transactions. The Controller's legal representative indicated that the complainant had lodged the complaint with the Commissioner primarily because the published data on financial transactions revealed misuse of the common funds of the trade union members and potential criminal offences attributable to the former management, which had exercised its managerial function on the basis of elections subsequently annulled by a final court judgment. The Controller had no knowledge of these financial abuses before publishing the account statements on its website, given that the lawful management regained access to the bank accounts only after seven years. The statements containing the published data were subsequently taken down by the web-hosting provider.

During the inspection, relevant documents and evidence confirming the Controller's status as a trade union organisation were obtained and, after the inspection, submitted to the authorised officer of the Commissioner.

Acting upon the said complaint and following the extraordinary inspection, the Commissioner issued a warning for the following reasons.na

The provisions of Article 5(1)(1)–(6) of the LPDP prescribe the principles of personal data processing, whereby personal data must: be processed lawfully, fairly and transparently in relation to the data subject, with lawful processing meaning processing carried out in accordance with this law or another law regulating the processing ("lawfulness, fairness and

transparency"); be collected for purposes that are specifically defined, explicit, justified and lawful, and must not be further processed in a manner inconsistent with those purposes ("purpose limitation"); be adequate, relevant and limited to what is necessary in relation to the purpose of the processing ("data minimisation"); be accurate and, where necessary, kept up to date, with all reasonable measures taken to ensure that inaccurate personal data are erased or rectified without delay ("accuracy"); be kept in a form that permits identification of the data subject for no longer than is necessary for the fulfilment of the purpose of the processing ("storage limitation"); and be processed in a manner that ensures appropriate protection of personal data, including protection from unauthorised or unlawful processing, as well as accidental loss, destruction or damage, through the application of appropriate technical, organisational and staffing measures ("integrity and confidentiality").

Paragraph 2 of the aforementioned Article of the LPDP prescribes that the controller is responsible for the application of the provisions of paragraph 1 of that Article and must be able to demonstrate their application ("accountability").

According to Article 12(1) of the LPDP (Lawfulness of processing), processing is lawful only if one of the following conditions is fulfilled:

1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes;
2) the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps, at the request of the data subject, prior to entering into a contract;
3) the processing is necessary for compliance with the controller's legal obligations;
4) the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller by law;
6) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring personal data protection, particularly where the data subject is a minor.

Article 17(1) of the LPDP prescribes that processing revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, is prohibited.

Paragraph 2 of the same Article of the LPDP stipulates that, exceptionally, the processing referred to in paragraph 1 of this Article is permitted in the cases listed under items 1) to 10).

In the course of the inspection oversight, it was established that the Controller, by making available on its website the account statements of the Controller's current account, disclosed personal data contained in the statements relating to transactions made to the accounts of natural persons.

It is undisputed that the Controller had a legitimate interest in ensuring transparency of financial flows. However, even in such circumstances, the Controller was obliged to ensure that only those data which do not identify or make identifiable natural persons are published, where the Controller has no legal basis for processing such data, regardless of the fact that the Controller was not aware that the statements contained transactions made to the accounts of natural persons.

It was taken positively that, immediately upon learning that the published data contained personal data, the Controller removed them from the official website without delay, thereby preventing any further disclosure of the data.

Having regard to the established facts and the circumstances under which the Controller's account statements were published, as well as the provisions of Articles 5, 12 and 17 of the LPDP, the Controller was under an obligation, prior to publishing the data on the official website, to verify whether the statements in question contained personal data of natural persons and whether there was a lawful basis for such processing within the meaning of Articles 12 and 17 of the LPDP. The Controller failed to carry out that verification, and the processing in question has, in the inspection oversight procedure, been found to be contrary to the provisions of the LPDP.

Case Number: 072-21-3258/2025-07

1.27. Processing of personal data of tenants by publishing a document in the Viber group of the residential community

From the operative part:

The Commissioner warned Residential Community X, as the controller of personal data, because the building manager of this residential community published, in the tenants' Viber group, the complaint submitted by tenant XY to the Court of Honour of the Serbian Chamber of Commerce, which, among other things, contained this individual's personal data. By doing so, the manager made this person's data available to an indeterminate number

of individuals without any lawful basis, thereby violating Article 5(1)(1) of the LPDP, that is, processing personal data in a manner contrary to the principle of lawfulness, fairness and transparency in relation to the data subject.

From the reasoning:

In the course of the inspection oversight, it was established, inter alia, that: the professional manager of Residential Community X published, in the tenants' Viber group, the complaint submitted to the Court of Honour of the Serbian Chamber of Commerce by tenant XY against him, which had subsequently been forwarded to him by the Court of Honour for his statement; that the said complaint submitted to the Court of Honour contained, among other things, the following personal data of tenant XY: full name, residential address, mobile telephone number and e-mail address.

Article 4(1) of the LPDP prescribes, inter alia, that personal data are any data relating to a natural person whose identity is determined or identifiable, directly or indirectly, in particular on the basis of an identity marker such as a name and identification number, location data, identifiers in electronic communications networks, or one or more characteristics of that person's physical, physiological, genetic, mental, economic, cultural or social identity; that a data subject is a natural person whose personal data are processed; that the processing of personal data means any operation or set of operations performed, whether by automated or non-automated means, on personal data or sets of personal data, such as disclosure, access, use, disclosure by transmission or delivery, copying, dissemination or otherwise making available; and that a third party is a natural or legal person, or public authority, which is not the data subject, controller or processor, nor a person authorised to process personal data under the direct authority of the controller or processor.

Article 5(1)(1) of the LPDP prescribes that personal data must be processed lawfully, fairly and transparently in relation to the data subject ("lawfulness, fairness and transparency"), and that processing is lawful when carried out in accordance with this law or another law governing the processing.

Article 12(1) of the LPDP prescribes that processing is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically determined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject, or for taking steps at the request of the data subject prior to entering into a contract; 3) the processing is necessary for compliance with the controller's legal obligations; 4) the processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) the processing is necessary for the performance of tasks carried out in the public interest or in the exercise of

powers prescribed by law and vested in the controller; 6) the processing is necessary for the purposes of the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where the data subject is a minor.

Article 15(1)(3) of the Law on Housing and Building Maintenance ("Official Gazette of the RS", Nos. 104/2016 and 9/2020 – other law, hereinafter: LH&BM) prescribes, inter alia, that building management is carried out by the housing community through its bodies, or by a professional manager entrusted with the management tasks.

Article 50(1) of the LH&BM prescribes the rights and obligations of the building manager of the housing community.

Article 54(2) of the Law on Housing and Building Maintenance prescribes, inter alia, that the Serbian Chamber of Commerce and Industry organises courts of honour for determining violations of professional standards and norms (professional responsibility), as well as for imposing measures for such violations. Paragraph 3 of the same article prescribes that the organisation and manner of performing the tasks referred to in paragraphs 1 and 2 of this Article are regulated in more detail by a general act of the Serbian Chamber of Commerce and Industry.

Article 24(1) of the Rules of Procedure of the Court of Honour of the Serbian Chamber of Commerce ("Official Gazette of the RS", No. 114/2017) prescribes that a complaint regarding a violation of good business practice and business ethics shall be submitted to the prosecutor of the Court of Honour. Article 27 of the same Rules prescribes that proceedings before the Court of Honour are initiated by a request submitted by the prosecutor, while Article 32 prescribes that the request shall be delivered to the business entity with an invitation to submit a response to the Court of Honour within eight days.

Having regard to the above provisions of the LPDP, and bearing in mind that no provision of the Law on Housing and Building Maintenance grants the professional building manager the authority to disclose to a third party the personal data of the person who filed a complaint for a breach of good business practice and business ethics, the Controller, in the manner described above, by disclosing in the Viber group of the residential community the personal data of the complainant – namely the individual's full name, residential address, mobile phone number and e-mail address – carried out the processing of that individual's personal data contrary to the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP, without meeting any of the conditions for lawful processing set out in Article 12 of the same law.

Case Number: 072-21-2388/2024-07

1.28. The complainant states that he contacted the Police Directorate with a request to obtain data on suspected persons for the purpose of initiating court proceedings, and that, since he did not receive the requested data, he is requesting the Commissioner to issue a decision ordering the Ministry of the Interior to provide the requested data to the complainant.

From the opinion of the Commissioner:

Article 4(1)(1) of the Law on Personal Data Protection prescribes that personal data are any data relating to a natural person whose identity is determined or identifiable, directly or indirectly, in particular on the basis of an identity marker such as a name or identification number, location data, identifiers in electronic communications networks, or one or more characteristics of that person's physical, physiological, genetic, mental, economic, cultural or social identity.

As a general observation, we note that, pursuant to Article 12 of the Law on Personal Data Protection, the processing of personal data is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject or in order to take steps at the request of the data subject prior to entering into a contract; 3) the processing is necessary for compliance with a legal obligation of the controller; 4) the processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of powers prescribed by law and vested in the controller; 6) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where the data subject is a child.

Thus, the processing of personal data is lawful only if it is carried out in accordance with the Law on Personal Data Protection (LPDP) or another law governing the specific processing of data. Furthermore, for the processing of data to be lawful, in addition to having a legal basis, there must be a defined, justified and lawful purpose; only data that are adequate, relevant and limited to what is necessary for achieving the purpose of the processing may be processed; the data may be stored in a form that enables the identification of the data subject only for as long as is necessary for achieving the purpose of the processing; appropriate protective measures must be taken against unauthorised and unlawful processing; and the other principles of processing prescribed by Article 5(1) of the LPDP must be applied.

Having regard to the content of the submission, it was indicated that the Law on Police ("Official Gazette of the RS", Nos. 61/2016, 24/2018 and 87/2018) prescribes, inter alia, police duties and powers, while the processing of personal data in the area of internal affairs and the exchange of data is governed by the Law on Records in the Field of Internal Affairs ("Official Gazette of the RS", No. 24/2018). Accordingly, the Commissioner, having regard to the prescribed competences, cannot influence police duties and powers established by these laws, nor can the Commissioner assess the actions of the Ministry of Interior in the specific case.

Therefore, bearing in mind that the Law on Personal Data Protection protects the rights of data subjects, it was noted that the data requested by the complainant concerning other persons, for the purposes of initiating civil proceedings, cannot be the subject of exercising any right under this law. As no infringement of the Law on Personal Data Protection has occurred in the present case, the complainant was informed that there is no basis for undertaking inspection or other actions within the competence of the Commissioner.

Case Number: 072-21-2511/2025-07

1.29. Handling a citizen's complaint concerning the lawfulness of the processing of personal data of building managers

The Commissioner received a citizen's complaint concerning the lawfulness of the processing of personal data of building managers, carried out by publishing their Unique Master Citizen Numbers (JMBG) within the portal Unique Register of Residential Communities on the official website of the Republic Geodetic Authority.

Article 4(1) of the LPDP prescribes that personal data means any information relating to a natural person whose identity is determined or identifiable, directly or indirectly, particularly on the basis of an identity marker, such as a name or an identification number, location data, identifiers in electronic communications networks, or one or more features of that person's physical, physiological, genetic, mental, economic, cultural or social identity. The same Article prescribes that the "data subject" is a natural person whose personal data are processed, and that "processing of personal data" (hereinafter: processing) means any operation or set of operations performed, whether automated or non-automated, on personal data or sets of personal data, such as collection, recording, sorting, grouping or structuring, storage, adaptation or alteration, disclosure, access, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, comparison, restriction, erasure or destruction.

Article 5(1)(1) of the LPDP prescribes that personal data must be processed lawfully, fairly and transparently in relation to the data subject ("lawfulness, fairness and transparency"), and that processing is lawful when carried out in accordance with this law or another law governing the processing.

Article 12(1)(3) of the LPDP prescribes that processing is lawful if it is necessary for compliance with the controller's legal obligations.

Article 20 of the Law on Housing and Building Maintenance ("Official Gazette of the RS", Nos. 104/2016 and 9/2020 – other law; hereinafter: the Law on Housing) prescribes, inter alia, that the Register of Residential Communities (hereinafter: the Register) is an electronic public database of data and documents containing the information on residential communities prescribed by this law and the by-laws on the Register adopted pursuant to this law. The Register particularly contains the following data which are registered, recorded and published: 1) the business name and the address of the residential community; 2) identification data on the building manager, namely, for a domestic natural person: name, surname and JMBG, and for a foreign natural person: name, surname, passport number and the issuing country; 3) identification data on the professional building manager and the organiser of professional management, namely, for a natural person: name, surname and JMBG; for a foreign natural person: name, surname, passport number and issuing country; and for a legal entity: business name, registered office address, registration number and tax identification number; 4) the registration number of the residential community; 5) the tax identification number of the residential community; 6) the current account number of the residential community and contact details (telephone number and e-mail address); 7) other data in accordance with the law and the act on the Register.

Article 21 of the Law on Housing prescribes, inter alia, that the Republic Geodetic Authority maintains a unified, central, public electronic database containing consolidated data on residential communities from all registers on the territory of the Republic of Serbia (hereinafter: the Unified Register of Residential Communities).

Article 36(4) of the Law on Housing prescribes that, after control of the accuracy of the data and documents entered into the central information system has been performed, the registered data and documents on a residential community shall be publicly published in the Unified Register of Residential Communities.

Article 4(1) of the Rulebook on the Contents of the Register and the Documentation Required for the Registration and Recording of Data on Residential Communities, as well as the Manner of Submitting Data and Documents ("Official Gazette of the RS", No. 49/2017), prescribes, inter alia, that the Register contains the following data on a residential community which are to be registered and published: 1) the business name of the residential community; 2) the address of the residential community (mu-

nicipality, settlement, street, house number; if the residential community is formed for several entrances, all house numbers must be stated); 3) the registration number of the residential community; 4) identification data on the building manager, namely, for a domestic natural person: name, surname and JMBG, and for a foreign natural person: name, surname, passport number and issuing country; 5) identification data on the professional building manager and the organiser of professional management, namely, for a domestic natural person: name, surname and JMBG; for a foreign natural person: name, surname, passport number and issuing country; and for a legal entity: business name, registered office address, registration number and tax identification number.

By examining the official website of the Republic Geodetic Authority – the Unified Register of Residential Communities https://katastar.rgz.gov.rs/StambeneZajednice/ (the link provided in the attachment to the submission), it was established that, by selecting a municipality from the drop-down list or by entering an address and/or the registration number of a residential community, it is possible, within the sub-menu Unified Register of Residential Communities → Overview of data on the residential community, in the section "Registrar's Decisions", to search the published decisions on the registration of residential communities and the conclusions on rejected registrations, and to inspect those acts. By examining an example of a decision on the registration of a residential community in the Register, i.e. a decision approving the registration request for the amendment of data in the Register of Residential Communities, it was established that such decisions, inter alia, contain the name, surname, and JMBG of the building manager who is entered into, or removed from, the relevant register.

Having regard to the above, it was established that the publication of the JMBG of building managers within the Unified Register of Residential Communities is carried out in accordance with the above-quoted provisions of the Law on Housing and Building Maintenance (ЗСО3), thereby fulfilling the condition for lawful processing prescribed by Article 12(1)(3) of the LPDP.

Case Number: 072-21-669/2024-07

1.30. Processing of personal data that are not part of a data filing system nor intended to form part of a data filing system

The Commissioner received a complaint stating that, in a certain retail establishment, a product had been accidentally knocked over and broken, after which the store employees insisted that the broken product be paid for. In connection with this, an employee of the Controller allegedly

retained the complainant's driving licence and recorded certain personal data on a sheet of paper.

Having regard to the allegations contained in the received complaint and the written statement submitted by the Controller, the Commissioner initiated a procedure for extraordinary inspection oversight regarding the application of the LPDP.

The subject of the extraordinary inspection oversight was the processing of personal data in situations involving the accidental damage or destruction of goods in a retail establishment by a visitor/customer.

During the inspection oversight, representatives of the Controller stated that "every breakage is treated internally and no personal data are taken from a potential customer… in this situation, at the moment of breakage, the complainant voluntarily left her driving licence so that, after withdrawing the necessary funds, she could return to the retail establishment and pay for the pitcher, which the Controller did not request; since, had she refused to pay, they would not have held her liable nor would they have requested her personal data."

The Controller further stated that it does not process personal data in such situations, since potential customers/clients are under no obligation to pay for damage in cases of accidental breakage or damage to an item, and that no records are kept in that regard.

It also stated that no receipt was issued because the complainant did not pay for the goods/item, and therefore a receipt could not have been issued. The leaving of the driving licence by the individual was done on her own initiative, and in that situation only the name and surname were noted, but such data were not further processed or stored. In this particular case, the employee assessed that, upon returning to the retail establishment, the complainant behaved discourteously and inappropriately and that a certain physical contact and attempt to take back the driving licence occurred. The employee then, out of concern that the situation might escalate into a more serious verbal or physical conflict, recorded the data, given previous situations in the retail establishment in which employees had been exposed to various threats. In this case, there was a misunderstanding in communication, given that a potential customer does not bear the cost of damage in the event of accidental damage or breakage of an item.

In addition, the Controller provided the authorised representative of the Commissioner with a document labelled as a "clarification" from the Director of the E-commerce Sector, stating that they do not have a consolidated customer database as such.

Attached was also evidence in the form of a "print screen" from a database containing a large number of users, showing that a search by the name and surname of the complainant returned "No Results Found".

The Controller also submitted to the Commissioner the document titled "Procedure in the event of unintentional damage to goods by a customer", which states the following:

"By this notice we inform you of the company's official policy regarding unintentional damage that customers may cause while present on the premises. Customers DO NOT bear responsibility for accidentally broken or damaged goods in the establishment, provided it is an unintentional incident. Our rules are as follows: Unintentional damage is not charged; If a customer accidentally knocks over, breaks or otherwise damages a product — without malicious intent — the customer must not be held liable for the resulting damage; Employees must not reprimand, pressure or treat the customer in an unpleasant manner in such situations; Courtesy, understanding and professionalism are mandatory, even when damage occurs; Employees are required to inform a superior or shift manager about the incident, without causing discomfort to the customer; The customer may be thanked for understanding, but no compensation should be demanded from them. If the customer offers to pay, they should be politely informed that this is not necessary; It is not permitted to take personal data or personal documents from the customer as collateral for compensation of damage - We aim to maintain a professional relationship with customers, without any need to burden them; You are required to report the damage to Business Control and your superior for further instructions - Colleagues will provide all further steps you must follow. Depending on the level of damage, the goods may be sold at an outlet price or written off to the service warehouse."

In addition, the Controller informed the Commissioner about the Notice provided to customers, which contains the following wording:

"We would like to inform you that you are not responsible for any unintentional damage that may occur during your visit to our premises. In the event that a product is accidentally broken, damaged or knocked over through an unintended action, we will not charge you for the resulting damage..."

In relation to the above, the Commissioner took into consideration Article 3(1) of the LPDP, which prescribes that this law applies to the processing of personal data carried out, in whole or in part, by automated means, as well as to non-automated processing of personal data which form part of a filing system or are intended to form part of a filing system.

The disputed action of taking a personal document and recording the customer's name and surname by a single employee, without the Controller's knowledge or instruction, cannot be qualified as an act of processing personal data that form part of a filing system or are intended to form part of a filing system, which is a necessary condition for the application of the LPDP, whether the processing is automated or non-automated.

Case Number: 072-21-3336/2025-07

1.31. Processing of personal data by courts in the exercise of judicial powers

The Commissioner for Information of Public Importance and Personal Data Protection received a submission alleging the unauthorised collection and processing of personal data by a private prosecutor and his attorney, without "consent" or a "legal basis", from the data subject's public Facebook profile. It was stated that they "took and processed photographs" showing the data subject's image, "copied other posts" containing the person's name, surname and other data, as well as "copied a video recording" allegedly containing the person's voice. All of these data were processed, copied and submitted as evidence in court proceedings.

In relation to the Commissioner's competence in the area of personal data protection, as established by the Law on Personal Data Protection (LPDP), it should be noted that Article 77(1) LPDP prescribes that the Commissioner exercises its powers, in accordance with the LPDP, on the territory of the Republic of Serbia, and in doing so acts in accordance with the law governing general administrative procedure, as well as, by analogy, the law governing inspection oversight, unless otherwise provided by the LPDP. Article 77(2) LPDP explicitly provides that the Commissioner is not competent to supervise processing carried out by courts in the exercise of their judicial powers.

In this regard, it should be noted that the Criminal Procedure Code establishes rules aimed at ensuring that no innocent person is convicted, and that a criminal sanction is imposed on the perpetrator of a criminal offence under the conditions prescribed by criminal law, on the basis of a lawfully and fairly conducted procedure.

With respect to the assessment of evidence and the establishment of facts, Article 16(1) of the Criminal Procedure Code prescribes that court decisions may not be based on evidence which, directly or indirectly, in itself or in the manner in which it was obtained, is contrary to the Constitution, this Code, another law, or generally accepted rules of international law and ratified international treaties, except in proceedings conducted for the purpose of obtaining such evidence (paragraph 1).

In this sense, Article 42 of the Constitution of the Republic of Serbia provides that the protection of personal data is guaranteed (paragraph 1); that the collection, holding, processing and use of personal data shall be regulated by law (paragraph 2); that the use of personal data outside the purpose for which they were collected, in accordance with the law, is prohibited and punishable, except for the purposes of conducting criminal proceedings or protecting the security of the Republic of Serbia, in the manner prescribed by law (paragraph 3); and that everyone has the right to be informed about the data collected on their person, in accordance with the law, and the right to judicial protection in case of their misuse (paragraph 4).

The evidence in criminal proceedings are regulated by Articles 82 to 187 of the Criminal Procedure Code. Article 82 of this Code prescribes that evidence in the proceedings shall be collected and presented in accordance with the provisions of this Code, as well as in any other manner provided by law. Article 83(1) of the Code, which concerns the subject of proof, stipulates that the subject of proof includes facts that constitute the elements of a criminal offence, or on which the application of another provision of criminal law depends. The subject of proof also includes facts on which the application of the provisions of criminal procedure depends (Article 83(2)). Facts shall not be proven if the court assesses that they are generally known, sufficiently discussed, admitted by the defendant in a manner that does not require further proof (Article 88), or if the parties' agreement on those facts is not contrary to other evidence (Article 83(3)). With respect to unlawful evidence, Article 84 of the Code prescribes that evidence obtained contrary to Article 16(1) of this Code (unlawfully obtained evidence) may not be used in criminal proceedings (paragraph 1). Unlawfully obtained evidence shall be removed from the case file, placed in a separate sealed envelope, and kept by the judge for preliminary proceedings until the final conclusion of the criminal proceedings, after which it shall be destroyed, and a record thereof shall be made (paragraph 2). By way of exception to paragraph 2, unlawfully obtained evidence shall be kept until the final conclusion of the court proceedings conducted due to the obtaining of such evidence (paragraph 3).

Furthermore, this Code establishes, as one of the special procedures, the summary procedure, within which it prescribes that an indictment proposal or private criminal complaint must contain: the defendant's name and surname, including personal data if known; a brief description of the act; the legal designation of the criminal offence; the designation of the court before which the main hearing is to be held; a proposal indicating which evidence should be presented at the main hearing, including an indication of the facts to be proven and the evidence proposed for such proof; and a proposal concerning the type and measure of criminal sanction and measures whose imposition is requested.

The question of whether a particular piece of evidence is lawful, relevant, and admissible in a specific court proceeding falls exclusively within the competence of the court conducting the proceedings, which is the authority that decides on the lawfulness of obtaining and presenting evidence.

In this regard, the Commissioner, as an independent supervisory authority, has no power to influence the work of the courts, nor to interfere with the question of the lawfulness of evidence in the proceedings, that is, to supervise the processing of personal data submitted, proposed, or presented before the court in the exercise of judicial powers.

In addition to the above, and without engaging in the circumstances of the specific case, we also refer to Article 17(1) and Article 17(2) items 5) and 6) of the Law on Personal Data Protection (LPDP).

That Article of the LPDP prohibits the processing of data revealing racial or ethnic origin, political opinion, religious or philosophical belief, or trade-union membership, as well as the processing of genetic data, biometric data for the purpose of unique identification of a person, data concerning health, or data concerning a natural person's sex life or sexual orientation (paragraph 1). Paragraph 2 prescribes that, by way of exception, the processing from paragraph 1 of this Article is permitted in the cases listed under items 1) to 10). Item 5) establishes the permissibility of processing personal data that the data subject has manifestly made public, while item 6) establishes the permissibility when the processing is necessary for the establishment, exercise, or defence of a legal claim, or when a court is acting within its jurisdiction.

Case Number: 072-21-4701/2025-07

1.32. Validity of the contract as a legal basis for the processing of personal data

The Commissioner received a complaint stating that the contract lists, as identification data, the unique personal identification number, name and surname, address details, telephone number, and the signatory to the contract, and that the signature on the contract is not that of the complainant. In the supplement to the complaint, it was indicated that the complainant learned of the contract and of the debts arising from it from an agency engaged in debt collection, and that an enforcement decision had also been received in connection with the debt in question.

In relation to the complaint in question, the Commissioner conducted an extraordinary desk-based inspection procedure and based on the facts and circumstances of the specific case, established the following.

With regard to the lawfulness of personal data processing, Article 12, paragraph 1 of the Law on Personal Data Protection prescribes that processing is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of his or her personal data for one or more specifically defined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject or for taking actions, at the request of the data subject, prior to the conclusion of the contract; 3) the processing is necessary for compliance with the controller's legal obligations; 4) the processing is necessary for the protection of the vital interests of the data subject or of another natural person; 5) the

processing is necessary for the performance of tasks carried out in the public interest or in the exercise of the controller's statutory powers; 6) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where the data subject is a minor.

Taking into account the established facts and the circumstances of the personal data processing, actions aimed at determining the existence and validity of a contract in the civil-law sense, or liability in the criminal-law sense, as well as the claim arising from these circumstances, do not fall within the Commissioner's competence, given that the matter essentially concerns an obligations-law issue between contracting parties. Establishing the existence and validity of a contract requires undertaking legal, evidentiary, and expert actions, including forensic examinations, which fall exclusively within the jurisdiction of competent courts and which the Commissioner is not authorised to determine in the course of acting upon a complaint.

Accordingly, since the core issue here is whether the complainant is a contracting party within the meaning of the Law on Obligations, the Commissioner could, only in a situation where a valid and legally binding contract exists, assess compliance by a given controller with the provisions of the Law on Personal Data Protection on the basis of Article 12, paragraph 1, item 2 of that Law ("the processing is necessary for the performance of a contract concluded with the data subject or for taking actions, at the request of the data subject, prior to the conclusion of the contract").

Case Number: 072-21-3444/2025-07

2. ACTION UPON THE COMPLAINT

The Commissioner for Information of Public Importance and Personal Data Protection acts upon complaints submitted by individuals alleging a violation of their rights in connection with the processing of personal data. The exercise of these rights is initiated by submitting a request to the data controller. If the controller fails to respond within 30 days from the date of submission of the request (or within the extended period of 60 days), or if the controller refuses the request, the conditions for submitting a complaint to the Commissioner are then met.

2.1. No erasure of personal data necessary for the fulfilment of the purpose of processing

From the reasoning:

On 7 March 2025, the Commissioner received a complaint from AA, submitted through BB, an attorney from Belgrade, alleging a violation of the right to the erasure of personal data by the Ministry of Internal Affairs of the Republic of Serbia as the data controller, following the request of 31 December 2024. In the complaint, he stated that the criminal proceedings conducted against him had been discontinued and that no sanction or measure had been imposed on him. He therefore considers that the Controller should have erased his data from the records it maintains on submitted criminal charges, pursuant to Article 30, paragraph 2, item 1 of the Law on Personal Data Protection.

In the response to the complaint dated 26 March 2025, the Controller adhered to the assertions set out in its reply No. 03.15.2 07-7-2/25 of 17 January 2025, which had been delivered to the complainant.

Article 30, paragraph 1 of the Law on Personal Data Protection prescribes that the data subject has the right to have his or her personal data erased by the controller, while paragraph 2 prescribes that the controller is obliged to erase, without undue delay, the data referred to in paragraph 1 of this Article in the following cases: the personal data are no longer necessary for the fulfilment of the purpose for which they were collected or otherwise processed; the data subject has withdrawn the consent on which the processing was based and there is no other legal basis for the processing; the data subject has lodged an objection to the processing in accordance with Article 37, paragraphs 1 and 2 of this Law; the personal data have been unlawfully processed; the personal data must be erased in order to comply with the controller's legal obligations; and when the personal data have been collected in connection with the provision of information society services referred to in Article 16, paragraph 1 of the Law.

Pursuant to Article 7, paragraph 1 of the Law on Records and Processing of Data in the Field of Internal Affairs, the Ministry is required to correct and update, without delay, any data found to be inaccurate, while paragraph 2 provides that the personal data collected and entered into records must be erased upon the expiry of the retention periods established by this or another law, or when it is established that the reasons for which the personal data were entered into the relevant records no longer exist.

Article 41, paragraph 1 of the same Law prescribes that, for the purpose of clarifying criminal offences, the Ministry shall maintain records and process data on natural and legal persons for whom there are grounds for suspicion that they have committed criminal offences, as well as data on the outcome of criminal prosecution. Paragraph 2 of the same Article

provides that the competent public prosecutor's office shall submit to the Ministry data on the outcome of criminal prosecution, including the dismissal of charges, extension of charges, reclassification of the criminal offence, withdrawal of prosecution, opportunity measures, and paragraph 8 of the same Article stipulates that such data constitute classified information, marked in accordance with the regulations on classified information, and shall be kept permanently.

In adopting its decision, the Commissioner took into account the established facts, as well as the provisions of the Constitution of the Republic of Serbia, the Law on Personal Data Protection, the Law on Records and Processing of Data in the Field of Internal Affairs, the Law on Juvenile Offenders and Criminal-Legal Protection of Minors, the Criminal Code, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data with its Protocols, ratified by the Republic of Serbia, and Recommendation R (87) 15 of the Committee of Ministers of the Council of Europe to member states.

Namely, in each individual case, when acting upon complaints, the Commissioner assesses whether the conditions have been met for the erasure of personal data from the Controller's records relating to submitted criminal charges, that is, whether the purpose of the processing has been fulfilled. In doing so, the Commissioner takes into account, following European practice, the following criteria: the necessity of retaining the data in light of the completion of an investigation; the final court decision, especially an acquittal; rehabilitation; the type and gravity of the criminal offence committed; the time elapsed since the commission of the criminal offence; the sanction imposed; and similar considerations.

Taking into account that in 2023 the complainant, as a minor, committed the criminal offence with which he had been charged – unauthorised possession of narcotic drugs under Article 246a, paragraph 1 of the Criminal Code – and that the court discontinued the criminal proceedings on 8 October 2024 due to the inadvisability of imposing educational measures, given that the complainant appeared for the first time as the perpetrator of a criminal offence and admitted its commission, the Commissioner finds that, at this point in time, the statutory conditions for the erasure of his personal data have not been met. Specifically, the present case cannot be equated with a situation where a criminal charge has been dismissed or criminal proceedings discontinued due to the absence of grounds for suspicion that the person committed the criminal offence, or where an acquittal has been rendered. Considering that Article 41, paragraph 1 of the Law on Records and Processing of Data in the Field of Internal Affairs prescribes that the purpose of maintaining records and processing data on natural persons for whom there are grounds for suspicion that they have committed criminal offences, as well as data on the outcome of criminal prosecution,

is to clarify criminal offences, the further processing of the data relating to the criminal charge in question is still necessary for achieving this purpose. Accordingly, such processing is not contrary to the principle of "storage limitation" set out in Article 5 of the Law on Personal Data Protection, which provides that personal data must be stored in a form that enables the identification of the data subject only for the period necessary to achieve the purpose of the processing.

Taking the above into account, the Commissioner finds that, at this time, the conditions for the erasure of data prescribed by Article 30, paragraph 2 of the Law on Personal Data Protection have not been met.

Nevertheless, this decision of the Commissioner does not relieve the Controller of the obligation to act in accordance with Article 7, paragraph 2 of the Law on Records and Processing of Data in the Field of Internal Affairs, which prescribes that personal data collected and entered into records must be erased when it is established that the reasons for which the personal data were entered into the relevant records no longer exist, as well as Article 8, paragraphs 2 and 3 of the Law on Personal Data Protection, which prescribe that, where personal data are processed by competent authorities for specific purposes, a deadline must be determined for when those data will be erased, or a deadline for a periodic assessment of the need for their retention. If such a deadline is not determined by law, it shall be determined by the controller, taking into account the necessity of the processing for operational purposes in a democratic society.

Accordingly, on the basis of Article 78, paragraph 1, item 6, in connection with Article 77, paragraph 2 of the Law on Personal Data Protection, and Article 136, paragraph 1 of the Law on General Administrative Procedure, the Commissioner has decided as set out in the operative part of this decision.

Case Number: 072-16-2393/2025-06

2.2. Exercising Rights in Relation to the Termination and Processing of Personal Data

From the reasoning:

AA submitted a complaint to the Commissioner through his authorised representative, BB, an attorney from Novi Sad, alleging, inter alia, a violation of the right to the erasure of personal data and requesting the termination of processing by the company Philips doo Belgrade–New Belgrade, in connection with his request of 8 May 2025 for the exercise of rights relating to personal data processing. He claimed that the Controller had refused to cease processing after he had lodged an objection and had continued

processing by sending automated messages to the complainant's mobile telephone via the "WhatsApp" application, despite having sent a response and an apology, as well as a promise to stop such actions.

In the Controller's statement on the complaint, dated 23 July 2025, it was noted, inter alia, that the Controller processes personal data in accordance with the Law on Personal Data Protection and with its Privacy Policy available on its website; that the complainant had initially contacted the Controller regarding an issue with a purchased device on 23 April 2025 via WhatsApp, and later by telephone and e-mail, and that the issue had been resolved on 29 April 2025. It further stated that on 8 May 2025 the complainant informed the Controller of a problem with the continued WhatsApp messages, requesting that the Controller stop sending them, and that the Controller acknowledged receipt of the notice on the same day and forwarded the matter to the team responsible for resolving such issues. The Controller stated that its WhatsApp customer support was provided by its subcontractor Sprinklr, a New York-based company specialising in digital solutions for customer support, and that the Controller relied on this system and was therefore not aware that the automated messaging problem persisted until the complainant's notification of 8 May 2025. It further stated that, as no additional complaints were received from the complainant, the Controller was unaware that the automated messages continued until it received a lawsuit on that matter on 30 June 2025. Upon re-examining the case, the Controller established that there had been a malfunction in the system developed by Sprinklr, which made it appear as though the complainant's device issue had not been resolved, thus triggering automated messages. The Controller indicated that, once the problem was identified, it was promptly resolved and the automated messages ceased after 30 June 2025. It also noted that the malfunction had concealed the WhatsApp conversation from the Controller's customer support agent. The Controller emphasised that the complainant had only requested that the automated messages be stopped and had not requested that his personal data be erased.

Pursuant to Article 21, paragraph 3 of the Law on Personal Data Protection, the controller is required, inter alia, to provide the data subject with information on the action taken on the basis of the request without delay, and no later than 30 days from the date of receipt of the request; while paragraph 4 stipulates that, if the controller does not act upon the request of the data subject, it must inform that person, without delay and no later than 30 days from the date of receipt of the request, of the reasons for not acting, as well as of the right to lodge a complaint with the Commissioner or to bring an action before the court.

Article 37, paragraph 1 of the Law on Personal Data Protection prescribes that, if the data subject considers it justified in relation to his or her particular situation, he or she has the right, at any time, to submit to the

controller an objection to the processing of his or her personal data carried out pursuant to Article 12, paragraph 1, items 5) and 6) of this Law, including profiling based on those provisions. The controller is obliged to cease processing the data of the person who has submitted the objection, unless it demonstrates that there are legal grounds for processing which override the interests, rights or freedoms of the data subject, or which are related to the submission, exercise or defence of a legal claim.

Article 101, paragraph 1 of the Law on General Administrative Procedure stipulates that the procedure shall be discontinued if the authority finds that there are no grounds for continuing it, and the law does not require its continuation.

Since the complainant's request relates solely to the exercise of the right to the termination of processing (right to object) under Article 37 of that Law, and not to the right to the erasure of data, a complaint to the Commissioner, pursuant to Article 82 of the same Law, may be submitted only due to the failure to act upon that request. Therefore, the complaint alleging a violation of the right to the erasure of personal data by the Controller is unfounded. Accordingly, on the basis of Article 78, paragraph 1, item 6, in connection with Article 77, paragraph 2 of the Law on Personal Data Protection, and Article 136, paragraph 1 of the Law on General Administrative Procedure, the Commissioner has decided as set out in the operative part of this decision.

Taking into account that the complainant, inter alia, lodged a complaint due to the Controller's failure to act upon his objection, that is, his request to terminate the processing of personal data – his mobile telephone number – through the WhatsApp application by sending messages, and that the Controller, although it had previously taken measures to act upon the request, but whose implementation had not occurred due to a technical error of which the Controller was not aware, took additional measures immediately upon learning that the processing had not been terminated and ceased further processing of the complainant's personal data by sending WhatsApp messages to his mobile telephone number, the Commissioner finds, in the present case, on the basis of Article 78, paragraph 1, item 6 of the Law on Personal Data Protection and Article 101 of the Law on General Administrative Procedure, that there are no grounds for continuing the procedure concerning the complaint submitted for violation of the right to the termination of processing.

Case Number: 072-16-3415/2025-06

2.3. No Grounds for Erasure of Personal Data Due to the Controller's Legal Obligation

From the reasoning:

On 21 October 2025, the Commissioner for Information of Public Importance and Personal Data Protection received a complaint from AA alleging a violation of the right to the erasure of personal data by "Balkan Bet" d.o.o. Belgrade, as the data controller, following his request of 22 October 2025. In the complaint, he stated that the Controller had refused to delete his data, referring to the Law on the Prevention of Money Laundering and the Financing of Terrorism, and had also refused to deactivate his user account without his prior physical presence at a payment point and the completion of a form, which he considers an excessively complicated procedure.

In its response to the complaint dated 12 November 2025, the Controller maintained the statements made in its reply to the complainant of 22 October 2025 and added that, as of the date of its response, the complainant had not completed any of the prescribed forms, and therefore the Controller was unable to deactivate the account or perform a "self-exclusion" of the account. It further stated that it could not erase the complainant's data even after account deactivation because it is an obliged entity under the Law on the Prevention of Money Laundering and the Financing of Terrorism and the Law on Games of Chance. The Controller also noted that the complainant's e-mail address had been removed from its marketing distribution lists.

Article 12, paragraph 1, item 5 of the Law on Personal Data Protection prescribes, inter alia, that processing is lawful if it is necessary for the performance of the controller's statutory powers.

Article 21, paragraph 1 of the same Law prescribes, inter alia, that the controller is obliged to take appropriate measures to provide the data subject with all information relating to the exercise of the rights referred to in Article 30 of this Law in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Article 30, paragraph 1 of the Law on Personal Data Protection prescribes that the data subject has the right to have his or her personal data erased by the controller, while paragraph 2 prescribes that the controller is obliged to erase, without undue delay, the data referred to in paragraph 1 of this Article in the following cases: the personal data are no longer necessary for the fulfilment of the purpose for which they were collected or otherwise processed; the data subject has withdrawn the consent on which the processing was based and there is no other legal basis for the processing; the data subject has lodged an objection to the processing in accordance with Article 37, paragraphs 1 and 2 of this Law; the personal data have been unlawfully processed;

the personal data must be erased in order to comply with the controller's legal obligations; and when the personal data have been collected in connection with the provision of information society services referred to in Article 16, paragraph 1 of the Law.

The provisions of the Law on the Prevention of Money Laundering and the Financing of Terrorism ("Official Gazette of the RS", Nos. 113/2017, 91/2019, 153/2020, 92/2023, 94/2024, 19/2025) prescribe, inter alia, that an obliged entity, within the meaning of this Law, includes organisers of special games of chance in gaming establishments and organisers of games of chance through electronic communication means (Article 4); that an obliged entity must retain data and documentation relating to the customer, the established business relationship with the customer, the risk assessment performed and the executed transaction, obtained in accordance with this Law, as well as the customer's file, business correspondence and the results of any analysis carried out in relation to the customer, for five years from the date of termination of the business relationship, execution of the transaction, or from the last access to the safe-deposit box or entry into the gaming establishment (Article 95, paragraph 1); that the obliged entity must handle the data referred to in paragraphs 1–3 of that Article in accordance with the law governing personal data protection and must erase those data upon expiry of the periods referred to in paragraphs 1 and 3 (Article 95, paragraph 4); and that, by way of exception to paragraph 4 of that Article, the obliged entity may retain or otherwise process the data referred to in that paragraph after the expiry of the periods referred to in paragraphs 1 and 3 only if the data are used by competent state authorities for specific purposes within the meaning of the Law referred to in that paragraph (Article 95, paragraph 5).

Article 11 of the Law on Games of Chance ("Official Gazette of the RS", Nos. 18/2020, 94/2024) prescribes, inter alia, that for the purpose of performing tasks in the public interest and exercising statutory powers, the Administration, in the procedure and in the manner prescribed by this Law, collects personal data either by submission from the organiser or the person referred to in Article 115 of this Law, or by directly accessing the data of the organiser or the person referred to in Article 115. These data include the personal data contained in an identity card or passport, such as the player's name, surname, identity-card or passport number, unique personal identification number, date and place of birth, and place of residence or domicile; audio and video recordings from premises where games of chance are organised; data on the location, time, amount, method and destination of transfers of prizes in goods and services; payments, withdrawals, stakes, winnings or losses of players; data on players' registration and promotional accounts; as well as data relating to their self-exclusion (paragraph 6). It further prescribes that the personal data referred to in paragraphs 6 and

7 of this Article shall be stored and retained for the periods prescribed by this Law, but no longer than ten years from the date of: 1) termination of the business relationship between the organiser and the player, in the case of closure of the player's registration account, where the data relate to a player whose registration account has been closed; 2) the expiry of the organiser's licence, approval or consent for organising games of chance, for all other personal data collected from that organiser (paragraph 8).

The Rules on Organising Special Games of Chance via Electronic Communication Means of "Balkan Bet" d.o.o. Belgrade, No. 729 of 3 December 2024, published on the Controller's website, prescribe, inter alia, that the organiser of games of chance shall make available, within the application, a form through which the user may initiate the procedure for self-exclusion from play for a specified period or permanently. Self-exclusion, including permanent self-exclusion, takes effect if the user submits a written request to the organiser and completes the required self-exclusion form. During the period of self-exclusion, the user will have limited access to his user account and will not be able to place bets (Article 20, paragraph 1). The participant accepts these Rules, published on the organiser's website, during the registration process. Acceptance of the Rules by the user is recorded within the personal data of each registered user (Article 25).

Taking into account the content of the request, the Controller's response, the allegations in the complaint, and the cited statutory provisions, the Commissioner finds that the complaint is unfounded because the conditions for the erasure of data prescribed by Article 30, paragraph 2, item 5 of the Law on Personal Data Protection—requiring erasure in order to comply with the controller's legal obligations—have not been met. It is undisputed that the Controller has a statutory obligation, in accordance with the cited legal provisions, to retain users' data for ten years from the date of closure of the player's registration account, or five years from the termination of the business relationship. As the Controller, in its response to the request, informed the complainant of the procedure for account closure, and the complainant has not provided evidence of having acted in accordance with the Controller's instructions, there are no grounds for the erasure of the data held in the Controller's records. This is all the more so given that the Controller publicly informed users of the account-closure procedure through the Rules on Organising Special Games of Chance via Electronic Communication Means, published on its website, which the user accepted during the registration process.

Accordingly, on the basis of Article 78, paragraph 1, item 6, in connection with Article 77, paragraph 2 of the Law on Personal Data Protection and Article 136, paragraph 1 of the Law on General Administrative Procedure, the Commissioner has decided as set out in the operative part of this decision.

Case Number: 072-16-4596/2025-06

2.4. No Violation of the Right to Erasure of Personal Data that the Controller Is Legally Required to Retain Permanently

From the reasoning:

AA submitted a complaint alleging a violation of the right to the erasure of personal data by the Ministry of Internal Affairs of the Republic of Serbia, as the data controller (hereinafter: the Controller), following his request for the deletion of his data from the Register of Registered Weapons. He stated that he is the owner of an air rifle which, pursuant to Article 4 of the applicable Law on Weapons and Ammunition, falls under Category D weapons for which the Controller does not maintain records or process personal data of the owners of such weapons. He further stated that he continues to be listed in the Register of Registered Weapons as the owner of the said air rifle and, consequently, is obliged to report the registered weapon in the asset declaration submitted to the Internal Control Sector, as well as to store the weapon locked and inaccessible to others, and that checks may be carried out regarding how he stores it, even though he may gift it to any person over the age of 16.

He additionally stated that his data were processed under the provisions of the law applicable at the time the weapon was registered, and that the current law cannot be applied retroactively; that he is being discriminated against compared to other owners of Category D weapons who acquire such weapons now; that he cannot obtain a certificate confirming that he does not possess registered weapons; and that, given that his data were processed under provisions of a law that is no longer in force, he requests the Commissioner to take measures within his competence and order the deletion of his personal data.

In its response to the complaint, the Controller stated that, by checking the records of deactivated weapons, it established that the complainant had registered an air rifle in 1995 in accordance with the Law on Weapons and Ammunition that ceased to be in force on 5 March 2016, and that he had been issued a weapon certificate, registration number 11864. It further stated that, after the entry into force of the currently applicable Law on Weapons and Ammunition ("Official Gazette of the RS", Nos. 20/15, 10/19, 20/20, 14/22), the status of that weapon was classified in the electronic register, within the "Legally Possessed Weapons" application, in accordance with the categorisation prescribed by the current law, under which the air rifle belongs to Category D weapons, which may be held without reporting to the competent authority. The Controller also stated that Article 44, paragraph 1 of the Law on Weapons and Ammunition prescribes that the competent authority shall maintain, among other registers, a register of deactivated weapons, while paragraph 4 of the same Article prescribes that all registers shall be kept permanently and in electronic form. In view of these statutory provisions, the electronic register maintained by the Controller

contains, in addition to registered weapons, data on weapons previously recorded under earlier laws, as well as data on weapons whose status has changed, and which can no longer be considered active weapons and are therefore placed in the register of deactivated weapons. With reference to the complainant's assertion that he could not obtain a certificate confirming that he does not possess registered weapons, the Controller stated that, for weapons contained in the deactivated-weapons register, it may issue a certificate confirming that the weapon is recorded in that register.

Article 21, paragraph 1 of the Law on Personal Data Protection prescribes, inter alia, that the controller is obliged to take appropriate measures to provide the data subject with all information relating to the exercise of the rights prescribed by this Law in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Paragraph 4 prescribes that, if the controller does not act upon the request of the data subject, it must inform that person, without delay and no later than 30 days from the date of receipt of the request, of the reasons for not acting, as well as of the right to lodge a complaint with the Commissioner or to bring an action before the court.

Article 30, paragraph 1 of the Law on Personal Data Protection prescribes that the data subject has the right to have his or her personal data erased by the controller, while paragraph 2 prescribes that the controller is obliged to erase, without undue delay, the data referred to in paragraph 1 of this Article in the following cases: the personal data are no longer necessary for the fulfilment of the purpose for which they were collected or otherwise processed; the data subject has withdrawn the consent on which the processing was based and there is no other legal basis for the processing; the data subject has lodged an objection to the processing in accordance with Article 37, paragraphs 1 and 2 of this Law; the personal data have been unlawfully processed; the personal data must be erased in order to comply with the controller's legal obligations; and when the personal data have been collected in connection with the provision of information society services referred to in Article 16, paragraph 1 of the Law.

Article 4, paragraph 1, item 4 of the Law on Weapons and Ammunition prescribes that weapons are divided into four categories, whereby Category D includes: cold weapons; pepper sprays; electroshock devices; air weapons with kinetic energy below 10.5 J or projectile velocity below 200 m/s and a calibre of 4.5 mm or less; as well as string- or spring-powered weapons with a draw force of up to 450 N, or a draw weight of up to 101 pounds. Article 5, paragraph 4 of the same Law prescribes that Category D weapons may be acquired and held without a certificate and without reporting to the competent authority, in accordance with that Law.

Article 44, paragraph 1 of the same Law prescribes that the competent authority shall maintain the following records: applications submitted;

issued permits for the acquisition of weapons; certificates of medical fitness; registered weapons; seized and surrendered weapons; deactivated weapons; found weapons; weapons reported as missing; applications submitted and issued weapons licences and certificates of the registration of weapon possession; applications submitted and issued permits for the acquisition of essential weapon components; applications submitted and issued decisions on collector's permits; applications submitted and issued permits for carrying weapons; applications submitted and issued permits for the import and export of weapons across the state border; applications submitted and issued decisions on engaging in the trade of weapons and ammunition, training in handling firearms, repair and modification of weapons; applications submitted and issued permits for legal entities and entrepreneurs for the acquisition of weapons, essential components and ammunition; applications submitted and issued decisions on the transport of weapons, essential components and ammunition; applications submitted and issued decisions on ammunition reloading; applications submitted and issued permits for the import, acquisition, possession and carrying of weapons by members of foreign diplomatic and consular missions and foreign nationals; applications submitted and issued decisions on mediation in the trade of weapons and ammunition; and deactivated weapons. Paragraph 3, items 1) and 3) prescribe that these records contain data on natural persons, including: name and surname, unique personal identification number, date and place of birth, nationality, identity card or identification document number, address of residence or domicile, photograph, occupation, deregistration of residence due to relocation, temporary or permanent stay abroad and return from abroad, as well as their status in relation to the weapon; and data on weapons, including: type, make, model, calibre and serial number. Paragraph 4 prescribes that all such records shall be kept permanently and in electronic form.

Taking into account the established facts and the cited statutory provisions, the Commissioner finds that the complaint is unfounded and that there has been no violation of the complainant's rights, since the complainant requested the erasure of data that the Controller processes on the basis of statutory authorisations granted by the Law on Weapons and Ammunition and which the Controller is legally obliged to retain permanently.

The complainant's assertions that the applicable law provides no legal basis for further processing of the data; that Article 44 of the Law on Weapons and Ammunition applies only to data processed under the provisions of that law and cannot be applied retroactively; that he is thereby discriminated against compared with other owners of Category D weapons whose data are not processed by the Ministry of the Interior; and that he cannot obtain a certificate from the Controller confirming that he does not possess registered weapons, could not influence the decision in a different direction. This is because Article 44 of the Law on Weapons and Ammuni-

tion expressly prescribes that the Controller maintains, inter alia, records of deactivated weapons, and that the Controller processes the data relating to the air rifle in question within the application concerning legally held weapons. In accordance with the applicable law, the weapon has been categorised as belonging to Category D, which may be held without reporting to the competent authority, and due to the change in the weapon's status it is no longer considered active but is recorded in the register of deactivated weapons, for which the Controller issues certificates confirming that the weapon is recorded in that register.

In view of all the foregoing, and given that the complainant's personal data relating to the air rifle are processed and retained permanently in accordance with the applicable Law on Weapons and Ammunition in the register of deactivated weapons; that the weapon concerned is considered legal; and that it has been categorised in such a manner that it may be held without reporting to the competent authority, the Commissioner concludes that there has been no violation of the complainant's rights.

Case Number: 072-16-2517/2024-06

2.5. The Law on Personal Data Protection Does Not Apply to the Data of Deceased Persons From the reasoning:

AA submitted a complaint against the Home for the Elderly "Lena Lux", Belgrade – Kaluđerica, as the data controller (hereinafter: the Controller), alleging a violation of the right of access to personal data. In the complaint, she stated, inter alia, that she had sent a request to the Controller seeking information regarding the stay, documentation, payments and contract of her late grandmother, BB. The Controller replied that it had changed ownership on 1 September 2024, that it did not possess data relating to her stay in 2021, and that she had received no information from the Controller concerning 2022, 2023 or January 2024.

Article 2, paragraph 1 of the Law on Personal Data Protection prescribes that this Law ensures the protection of the fundamental rights and freedoms of natural persons, particularly their right to the protection of personal data.

Article 4, paragraph 1 of the Law on Personal Data Protection prescribes that personal data are any data relating to a natural person whose identity is determined or determinable, directly or indirectly, particularly on the basis of an identifier such as a name and identification number, location data, identifiers in electronic communication networks, or one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity.

Article 77, paragraph 2 of the Law on Personal Data Protection prescribes that, in exercising its powers, the Commissioner shall act in accordance with the law governing general administrative procedure, as well as with the corresponding application of the law governing inspection oversight, unless otherwise provided by this Law.

Article 92, paragraph 1, item 2 of the Law on General Administrative Procedure prescribes that the authority shall dismiss by decision a request initiating a procedure if it is not competent to decide on the administrative matter and cannot determine which authority is competent.

Given that the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18) does not apply to the personal data of deceased persons, the Commissioner has no competence to act upon a complaint submitted for the purpose of alleging a violation of the right of access to the personal data of the deceased BB.

Case Number: 072-16-2497/2025-06

2.6. The Controller is obliged to provide copies of the personal data it processes to the complainant, not to the Commissioner. From the reasoning:

AA submitted a complaint alleging a violation of the right of access to personal data by the Public Enterprise "Post of Serbia" Belgrade, as the data controller (hereinafter: the Controller). In the complaint, she stated that she had first requested, on the basis of Article 26 of the Law on Personal Data Protection, that the Controller provide her with copies of all relevant acts and records concerning her employment status (contracts, annexes, decisions, salary records, evaluations, disciplinary proceedings, absences). However, the Controller did not provide the requested data within the statutory 30-day deadline; instead, it informed her by letter that she already possessed some of the documents and sent her unreadable photographs of a screen showing absence data. It also sent scanned annexes and decisions on temporary transfers by e-mail, and only after her repeated request did she receive documentation relating to the disciplinary procedure initiated against her in 2019. She further stated that, in a subsequent request, she asked for documentation and information relating to her transfer from her position in BB to CC, that she had initiated a labour dispute before the Basic Court in ... in relation to that matter, and had contacted the Labour Inspectorate in ..., but that the Controller did not respond to that request. She therefore asked the Commissioner to order the Controller to provide her with copies of all requested documents and data relating to her transfer to CC.

In its response to the complaint, the Controller stated, inter alia, that the complainant had submitted a request to the Regional Unit "DD", which is an organisational unit of the Controller, seeking access to and copies of all data relating to her that are kept in the personnel records, and that she had received a reply No. …, to which data were attached concerning all her absences from the moment such records began to be kept electronically. It further stated that, following her renewed request, the Controller sent her a letter enclosing a photocopy of the documentation relating to the disciplinary proceedings conducted against her in 2019; that on … 2025 the complainant submitted a request for information on working hours and transport arrangements, and that she received a response to that request by e-mail on … 2025. Regarding the complainant's specific request that she be provided with the data and documents relating to her transfer from Post Office BB to Post Office CC, the Controller stated that, in addition to the Notice on the Offer to Conclude an Annex to the Employment Contract and Annex No. 13 to the Employment Contract, which had already been provided to the complainant, it holds documentation consisting of three memoranda, only one of which contains the complainant's personal data, and that this document was enclosed. The Controller further stated that the allegations in the complaint were unfounded, since the complainant had been provided with all documentation in its possession containing her personal data, namely: the employment contract together with all related annexes; the documentation relating to the disciplinary proceedings conducted in 2019; data concerning the records of her absences; as well as information regarding working hours and transport arrangements. The Controller therefore considers the complaint to be unfounded.

Article 4, paragraph 1, item 1 of the Law on Personal Data Protection prescribes, inter alia, that personal data are any data relating to a natural person whose identity is determined or determinable, directly or indirectly; item 2 prescribes that a data subject is a natural person whose personal data are processed; and item 3 prescribes, inter alia, that the processing of personal data means any operation or set of operations performed, whether automated or non-automated, on personal data.

Article 26, paragraph 1 of the same Law prescribes, inter alia, that the data subject has the right to request from the controller information as to whether his or her personal data are being processed and to have access to those data. Paragraph 3 of the same Article prescribes that the controller is obliged, upon the request of the data subject, to provide him or her with a copy of the personal data being processed.

Article 79, paragraph 2, item 3 of the same Law prescribes that the Commissioner may order the controller or the processor to act upon the data subject's request regarding the exercise of his or her rights under that Law.

Taking into account the established facts and the cited statutory provisions, the Commissioner finds that the complaint is well-founded. This is because the Controller did not provide the complainant, within the statutory time limit, with copies of the requested data relating to her (documents concerning her transfer from Post Office BB to Post Office CC). Since it is undisputed that, under Article 26, paragraph 3 of the Law on Personal Data Protection, the complainant has the right to receive copies of the data, and since this right may be restricted only in the cases prescribed by Article 40 of the same Law, and the Controller did not invoke any of those grounds, it has been assessed that a violation of the right of access to data, within the meaning of Articles 21 and 26 of the Law on Personal Data Protection, has occurred.

The Commissioner considered the Controller's assertion that, with respect to the complainant's request for copies of the data and documents relating to her transfer from Post Office BB to Post Office CC, beyond the documentation already provided with her employment contract and its annexes, it holds three memoranda, only one of which contains the complainant's personal data and which was submitted in the annex. However, these assertions were not relevant for reaching a different decision, given that the Controller is obliged, pursuant to Article 26 of the Law on Personal Data Protection, to provide the complainant — not the Commissioner — with a copy of the data it processes. Therefore, by submitting to the Commissioner a copy of the data relating to the complainant, the Controller did not fulfil its obligation.

Accordingly, the Commissioner finds the complaint well-founded and, on the basis of Article 79, paragraph 2, item 3, in connection with Article 77, paragraph 2 of the Law on Personal Data Protection and Article 136, paragraph 1 of the Law on General Administrative Procedure, has decided as set out in the operative part of this decision.

Case Number: 072-16-3720/2025-06

2.7. Personal data of third parties cannot be erased

From the reasoning:

The Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) received, on 30 June 2025, via the e-mail address ..., a complaint from AA, supplemented on 7 July 2025, alleging a violation of the right to the erasure of personal data by the company "Mozzart" doo Belgrade, as the data controller (hereinafter: the Controller). In the complaint, she stated that on 22 May 2025 the Controller had used her personal address ... without her knowledge or consent to

open an account on its website. She further stated that she uses two versions of her e-mail address, … and …, with and without a dot, both created on the Google platform and both containing her personal identification data, but that the Controller refused to act upon her request to delete the e-mail address …, i.e. to deactivate the account created without her knowledge and consent, even though it is undisputed that the Controller communicated with her via the address without the punctuation mark as well as via the address containing the dot.

In its response to the complaint dated 18 July 2025, the Controller stated that the communication issue arose from the fact that, on 22 May 2025, the complainant received via the Gmail platform an e-mail that the Controller had sent to its user at the address …, as a person whose identity and accuracy of the submitted data had been verified during the creation of the user account, in accordance with the powers and obligations prescribed by the Law on Games of Chance. The Controller further stated that it had requested the complainant to provide her unique personal identification number so that it could verify whether there had been a potential misuse of data, which the complainant refused to do, continuing instead to insist that her e-mail address had been misused, although it is identical to the address created by the user of the Controller's services. It added that it cannot be held responsible for any improper delivery of the e-mail that it sent to the correct e-mail address, that the two versions of the e-mail address are similar but belong to different persons, and that it does not process personal data relating to the person who is the user of the e-mail address … in its records. In support of this, the Controller submitted the player information used during the registration of the account created with the e-mail address …, namely: name and surname, username, unique personal identification number, mobile telephone number, identity card number, and residential address. It also submitted data on the date of registration, verification and self-exclusion, market, and time limit of the monetary bonus.

Article 1, paragraph 1 of the Law on Personal Data Protection prescribes, inter alia, that this Law regulates the right to the protection of natural persons with regard to the processing of personal data and the free movement of such data, the principles of processing, and the rights of data subjects. Article 2, paragraph 1 prescribes that this Law ensures the protection of the fundamental rights and freedoms of natural persons, particularly their right to the protection of personal data.

Article 4, paragraph 1, item 1 of the Law on Personal Data Protection prescribes that personal data are any data relating to a natural person whose identity is determined or determinable, directly or indirectly, particularly on the basis of an identifier such as a name or identification number, location data, identifiers in electronic communications networks, or one or more factors specific to that person's physical, physiological, genetic,

mental, economic, cultural or social identity. Item 2 prescribes that a data subject is a natural person whose personal data are processed.

Article 21, paragraph 1 of the Law on Personal Data Protection prescribes, inter alia, that the controller is obliged to take appropriate measures to provide the data subject with all information relating to the exercise of the rights referred to in Article 26 and Articles 29 to 31 of this Law in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Paragraph 3 of the same Article prescribes that the controller must provide the data subject with information on the action taken on the basis of the request referred to in Article 26 and Articles 29 to 31 without delay and no later than 30 days from the date of receipt of the request. This deadline may be extended by an additional 60 days, if necessary, taking into account the complexity and number of requests. Paragraph 4 prescribes that, if the controller does not act upon the request of the data subject, it must inform the person without delay, and no later than 30 days from the date of receipt of the request, of the reasons for not acting, as well as of the right to lodge a complaint with the Commissioner or to bring an action before the court.

Article 30, paragraph 1 of the Law on Personal Data Protection prescribes that the data subject has the right to have his or her personal data erased by the controller, while paragraph 2 prescribes that the controller is obliged, without undue delay, to erase the data referred to in paragraph 1 of this Article in the following cases: the personal data are no longer necessary for the fulfilment of the purpose for which they were collected or otherwise processed; the data subject has withdrawn the consent on which the processing was based and there is no other legal basis for the processing; the data subject has lodged an objection to the processing in accordance with Article 37, paragraphs 1 and 2 of this Law; the personal data have been unlawfully processed; the personal data must be erased in order to comply with the controller's legal obligations; and where the personal data have been collected in connection with the provision of information society services referred to in Article 16, paragraph 1 of the Law.

Article 102a, paragraph 1 of the Law on Games of Chance ("Official Gazette of the RS", Nos. 18/20 and 94/24) prescribes that, for the purpose of protecting minors and enforcing the prohibition on participation of minors in games of chance, an organiser of special games of chance via electronic communication means is obliged, at the time of registration of a player's account, to verify the age of the individual by inspecting the date of birth contained in that person's identification document using electronic communication means (player verification). Paragraph 3 prescribes, inter alia, that the detailed conditions and procedure for verification are determined by the Minister of Finance.

Article 2, paragraph 3 of the Rulebook on the Conditions and Procedure for Player Verification by Organisers of Special Games of Chance No.

001892580 2025 10520 027 000 012 001 of 28 April 2025 prescribes that, during player verification via electronic communication means, the organiser shall verify whether the person registering to participate in games of chance via electronic communication means holds a valid personal identification document (identity card or passport), and shall determine, by inspecting the date of birth in the identification document, that the person is of legal age.

Taking into account the content of the request, the Controller's reply, the allegations in the complaint, the Controller's statement, the evidence provided regarding the identity of the person who verified his user account, as well as the cited statutory provisions, the Commissioner finds that the complaint is unfounded. This is because the right to the protection of personal data under the Law on Personal Data Protection belongs to each natural person to whom the data relate. Since the complainant requested the erasure of data relating to a natural person who is a user of the Controller's services, the present case does not concern the exercise of rights in connection with the processing of the complainant's personal data within the meaning of Article 1, paragraph 1 and Article 4, paragraph 1, items 1) and 2) of the Law on Personal Data Protection.

The fact that the complainant bases her request for the erasure of another person's personal data on the circumstance that she is the user of an e-mail address similar to that of the Controller's service user—due to which she received all e-mails the Controller sent to its user—did not influence the decision. Although the name and surname contained in the e-mail … are unquestionably data relating to the complainant, those data are also data that the Controller collected and entered into its records, within its statutory competences, during the registration procedure conducted via electronic communication means, by verifying the identity of the individual through inspection of an identification document. Therefore, the Commissioner finds that the data whose erasure the complainant is requesting do not relate to her; that they were collected and processed for purposes specifically defined and prescribed by the Law on Games of Chance and the accompanying rulebook; and that they are not eligible for erasure because the conditions prescribed by Article 30 of the Law on Personal Data Protection have not been met—about which the Controller also informed the complainant.

The complainant's allegation that she uses two versions of her e-mail address, … and …, with and without a dot, and that even though the Controller has verified this beyond doubt, it still refused to delete the version without a dot, likewise had no bearing on the decision. This is because the Commissioner finds that the Controller acted diligently and with the due care of a prudent business operator in its correspondence with the complainant, directing her to report any potential misuse to the High-Tech

Crime Department of the Ministry of the Interior, and indicating that by providing an additional piece of personal information it could verify whether there had been any potential misuse of personal data relating to her.

Case Number: 072-16-3432/2025-06

2.8. The Controller may delete only those personal data relating to an individual that it holds

From the reasoning:

The Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) received, on 28 October 2025, with an addendum of 31 October 2025, a complaint submitted by AA through BB, an attorney from Novi Sad, alleging a violation of the right to the erasure of personal data by the Ministry of the Interior of the Republic of Serbia, as the data controller (hereinafter: the Controller), in relation to a request dated 26 September 2025. The complaint states that in 2011, when the complainant was a minor, an educational measure of warning and guidance—a judicial reprimand—was imposed on him, yet the Controller's register titled "Criminal Offences and Perpetrators" still contains a notation indicating that criminal proceedings were conducted against him, although fourteen years have passed since the measure was imposed. It is further stated that the complainant, as well as members of his family, are experiencing difficulties due to this notation. The complaint also states that, in response to his request for the erasure of personal data, the Controller informed him that the request should have been submitted to the Higher Court in Sombor. Given, however, that the register in question is kept by the Controller and not by the court, the complainant requests that the Commissioner order the Controller to erase the personal data relating to the notation indicating that criminal proceedings were conducted against him before the Higher Court in Sombor for the criminal offence under Article 246a of the Criminal Code.

In its statement dated 21 November 2025, the Controller maintained the arguments presented in its response No. 07-7-290/25 of 10 October 2025, which had been submitted to the complainant's legal representative, and added that the complainant's request did not seek the erasure of his data from the operational-criminal records prescribed under Article 41 of the Law on Records and Processing of Data in the Field of Internal Affairs. Given that the complainant's representative is an attorney, the Controller considered that there was no basis to instruct him to amend the request in accordance with Article 59 of the Law on General Administrative Procedure. The Controller also stated that it processes the complainant's data

in the operational-criminal records in connection with the criminal report No. KU 221/10 of 1 May 2010, filed against him on grounds of reasonable suspicion that he committed the criminal offence under Article 246a, paragraph 1 of the Criminal Code, and that the outcome of the criminal proceedings has not been entered in that record.

Article 21, paragraph 1 of the Law on Personal Data Protection prescribes, inter alia, that the controller must take appropriate measures to provide the data subject with all information related to the exercise of rights under Article 26 of that Law in a concise, transparent, intelligible and easily accessible manner, using clear and plain language.

Article 102, paragraph 1 of the Criminal Code of the Republic of Serbia ("Official Gazette of the RS", Nos. 85/05, 88/05 – corr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19 and 94/24) prescribes that the criminal records contain personal data on the perpetrator of a criminal offence, data on the criminal offence for which the person was prosecuted, data on the sentence, conditional sentence, judicial admonition, exemption from punishment and pardoned punishment, as well as data on the legal consequences of the conviction. Subsequent amendments to the data contained in the criminal records, data on the serving of the sentence, and the deletion of records relating to wrongful convictions, are also entered in the criminal records.

Article 37, paragraph 1 of the Law on Juvenile Offenders and Criminal Law Protection of Juveniles ("Official Gazette of the RS", No. 85/2005) prescribes that the record of educational measures and juvenile imprisonment imposed on a minor shall be kept by the court that adjudicated the case at first instance.

Article 41, paragraph 1 of the Law on Records and Processing of Data in the Field of Internal Affairs ("Official Gazette of the RS", No. 24/18) prescribes that, for the purpose of clarifying criminal offences, the Ministry shall maintain records and process data on natural and legal persons for whom there are grounds for suspicion that they have committed criminal offences, as well as data on the outcome of criminal prosecution. Paragraph 2 of the same Article prescribes that data on the outcome of criminal prosecution—namely dismissal of charges, extension of charges, reclassification of the criminal offence, withdrawal of prosecution, or diversion—shall be submitted to the Ministry by the competent public prosecutor's office. Paragraph 5 prescribes that data on imposed sentences, acquittals, conditional sentences, judicial admonitions, exemptions from punishment, pardoned punishments, legal consequences of conviction, deletion of records concerning wrongful convictions, fines, imposed educational measures, measures of enhanced supervision, compulsory treatment measures, and other security measures imposed in criminal proceedings shall be kept by the Ministry on the basis of information submitted by the competent courts.

Data on judgments and other sanctions imposed by foreign courts shall be kept on the basis of information submitted to the Ministry by the Ministry of Justice.

Taking into account the content of the request for the exercise of rights relating to personal data processing—in which the complainant sought the erasure of personal data from the criminal records concerning the outcome of the criminal proceedings conducted against him in 2011—the Controller's response stating that it does not process the complainant's data in the criminal records, the allegations in the complaint, the Controller's statement, and the cited legal provisions, the Commissioner finds that the complaint is unfounded and that, in the present case, there has been no violation of the complainant's rights. This is because the Controller informed the complainant that it does not process the data relating to him—namely, the outcome of the criminal proceedings in which an educational measure was imposed by the Higher Court in Sombor—in the criminal records from which the complainant sought erasure, as the Controller may erase only those data relating to an individual submitting the request that it actually holds.

In addition, the Controller informed the Commissioner that it does not hold, even within the operational-criminal records, any data relating to the outcome of the criminal proceedings conducted against the complainant for the criminal offence of unauthorised possession of narcotic drugs under Article 246a of the Criminal Code, based on criminal report No. KU 221/10 of 1 May 2010.

Therefore, on the basis of Article 78, paragraph 1, item 6), in connection with Article 77, paragraph 2 of the Law on Personal Data Protection, and Article 136, paragraph 1 of the Law on General Administrative Procedure, the Commissioner decided as stated in the operative part of this decision.

Case Number: 072-16-4649/2025-06

2.9. Personal data cannot be erased before the expiry of the statutory retention period

From the reasoning:

The Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) received, on 9 September 2025, a complaint submitted by AA and completed on 16 September 2025, lodged against the Ministry of the Interior of the Republic of Serbia as the data controller (hereinafter: the Controller), alleging a violation of his right to the erasure of personal data. In the complaint, he stated, inter alia, that the Controller had refused to erase his personal data from its records,

pursuant to his request of 23 July 2025. In its statement on the allegations in the complaint, set out in letter 3.29. No. 07-7-240/25 of 13 October 2025, the Controller stated, inter alia, that, acting upon the complainant's multiple requests, it had informed him that his personal data relating to a criminal offence were being processed in connection with criminal report No. KU 131/96 of 13 August 1996, concerning the criminal offence under Article 201, paragraph 3 of the Criminal Code, for which no outcome of the proceedings had been recorded. It further stated that his data relating to reported incidents of domestic violence were processed in the domestic violence prevention register under No. 16665/2020 of 10 August 2020, and that the right to access data and documentation concerning persons against whom domestic violence has been committed is not a right that may be exercised under the Law on Personal Data Protection. The Controller also stated that data on submitted criminal reports, together with information on the outcome of criminal prosecution, are stored permanently unless otherwise prescribed by law; that the erasure of data on submitted criminal reports cannot be equated with rehabilitation, as these concern different types of data and different legal institutes; that the outcome of criminal proceedings—dismissal of a criminal report, acquittal, or rehabilitation—does not constitute a ground for erasure, since the purpose of the operational-criminal records is to record submitted criminal reports and the outcomes of proceedings; and that the register is relevant solely for the operational work of the police. Accordingly, the Controller considers that no violation of the law has occurred and that the complaint is unfounded.

In the supplemental statement on the complaint, received by the Commissioner's Office on 14 November 2025, the Controller emphasised that data on reported cases of domestic violence are kept in accordance with Article 32 of the Law on the Prevention of Domestic Violence ("Official Gazette of the RS", Nos. 94/2016 and 10/2023 – other law), the Rulebook on Records and Documentation on Persons Against Whom Domestic Violence Has Been Committed and on Persons Against Whom Protective Measures Have Been Imposed ("Official Gazette of the RS", No. 88/2023), the Regulation on the Content and Manner of Keeping Records on Cases of Domestic Violence ("Official Gazette of the RS", No. 4/2017), the Law on the Police ("Official Gazette of the RS", Nos. 6/2016, 24/2018, 87/2018 and 86/2019), and the Law on Personal Data Protection. The Controller stated that the records kept by the police contain: 1) data on reported cases of domestic violence (participants in the event, time, place, collected statements, circumstances of the case, data on the potential victim, etc.); 2) data on the reported potential perpetrator (name, surname, unique citizen identification number, address of residence or temporary residence, data on previously imposed protective measures); 3) data on risk assessments and the names of authorities to which the risk assessment was submitted; 4) data

on the imposition of emergency measures (date and number of the order imposing emergency measures, their duration and commencement time); 5) data on the extension and enforcement of emergency measures (number and date of the basic court's decision extending the emergency measures, data on the enforcement of the emergency measures); 6) data on the enforcement of protective measures against domestic violence. It further stated that the purpose of processing these data is the prevention and suppression of domestic violence, risk assessment, protection of endangered persons, cooperation with other competent authorities—centres for social work, public prosecutors' offices, and courts—and ensuring effective protection of victims. Processing is carried out on the basis of Article 12, paragraph 1, item 3) and Article 8 of the Law on Personal Data Protection, as well as Article 5, paragraph 2 of the Law on the Police. The Controller added that the data are retained in accordance with Article 32, paragraph 11 of the Law on the Prevention of Domestic Violence, which prescribes that the data shall be kept for at least ten years, after which they shall be erased; that deletion of the data before the expiry of that period is not permitted if doing so would jeopardise the lawfulness of proceedings or violate the rights of the victim; and that the data are not publicly accessible and may be handled solely by authorised officials, with the application of all organisational and technical measures for the protection of personal data.

Following the examination of the complaint, a decision was adopted as stated in the operative part of this ruling, for the following reasons:

Article 34, paragraph 3 of the Constitution of the Republic of Serbia prescribes that every person shall be presumed innocent of a criminal offence until his or her guilt has been established by a final court decision. Article 42, paragraph 3 of the Constitution prescribes that the use of personal data for purposes other than those for which they were collected in accordance with the law is prohibited and punishable, except for the purposes of conducting criminal proceedings or protecting the Republic of Serbia.

Article 194, paragraph 3 of the Constitution of the Republic of Serbia prescribes that all laws and other general acts adopted in the Republic of Serbia must be in conformity with the Constitution, whereas paragraph 5 of the same Article prescribes that laws and other general acts adopted in the Republic of Serbia must not be contrary to ratified international treaties and generally accepted rules of international law.

Article 5, paragraph 1 of the Law on Personal Data Protection prescribes, inter alia, that personal data must be collected for purposes that are specifically defined, explicit, justified and lawful, and must not be further processed in a manner that is incompatible with those purposes ("purpose limitation"); that the data must be adequate, relevant and limited to what is necessary in relation to the purposes of processing ("data minimi-

sation"); and that they must be stored in a form that permits identification of the data subject only for as long as necessary to achieve the purpose of the processing ("storage limitation").

Article 30, paragraph 1 of the Law on Personal Data Protection prescribes that the data subject has the right to have his or her personal data erased by the controller, while paragraph 2 prescribes that the controller is obliged, without undue delay, to erase the data referred to in paragraph 1 of this Article in the following cases: the personal data are no longer necessary for the purpose for which they were collected or otherwise processed; the data subject has withdrawn the consent on which the processing was based and there is no other legal basis for the processing; the data subject has lodged an objection to the processing in accordance with Article 37, paragraphs 1 and 2 of this Law; the personal data have been unlawfully processed; the personal data must be erased in order to comply with the controller's legal obligations; and where the personal data have been collected in connection with the provision of information society services referred to in Article 16, paragraph 1 of the Law.

Article 32, paragraph 1 of the Law on Personal Data Protection prescribes that, where processing is carried out by competent authorities for special purposes, the data subject has the right to have his or her personal data erased by the controller, and the controller is obliged, without undue delay, to erase those data if the processing has infringed the provisions of Articles 5, 13 and 18 of this Law, or if the personal data must be erased in order to meet the controller's legal obligations.

Article 79, paragraph 2, item 7) of the Law on Personal Data Protection prescribes, inter alia, that the Commissioner may order the erasure of personal data in accordance with Articles 29 to 32 of that Law.

Article 100 of the Law on Personal Data Protection further prescribes that the provisions of other laws relating to the processing of personal data must be harmonised with the provisions of that Law by the end of 2020.

Article 7, paragraph 1 of the Law on Records and Processing of Data in the Field of Internal Affairs prescribes that the Ministry is obliged to correct and update, without delay, any data found to be inaccurate, while paragraph 2 prescribes that collected personal data entered into records must be erased upon the expiry of the retention periods established by that or another law, or when it is established that the reasons for entering the personal data into the corresponding records no longer exist.

Article 41, paragraph 1 of the same Law prescribes that, for the purpose of clarifying criminal offences, the Ministry keeps records and processes data on natural and legal persons for whom there are grounds for suspicion that they have committed criminal offences, as well as data on the outcome of criminal prosecution. Paragraph 2 of the same Article prescribes that data on the outcome of criminal prosecution—namely

dismissal of charges, extension of charges, reclassification of the offence, withdrawal of prosecution, or diversion—shall be submitted to the Ministry by the competent public prosecutor's office. Paragraph 8 prescribes that such data constitute classified information, to be marked in accordance with regulations on classified information, and that they shall be stored permanently.

Article 97, paragraph 1 of the Criminal Code ("Official Gazette of the RS", Nos. 85/2005, 88/2005 – corr., 107/2005 – corr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 and 94/2024) prescribes that rehabilitation annuls the conviction and terminates all its legal consequences, and the convicted person shall be regarded as not having been convicted.

The Law on the Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Official Gazette of the FRY – International Treaties", No. 1/92; "Official Gazette of SCG – International Treaties", No. 11/2005 – other law; and "Official Gazette of the RS – International Treaties", Nos. 98/2008 – other law and 12/2010) and the Law on the Ratification of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Official Gazette of the RS – International Treaties", No. 4/2020) prescribe that personal data undergoing processing shall, inter alia, be collected for explicit, specified and legitimate purposes and shall not be processed in a manner incompatible with those purposes; that they shall be adequate, relevant and not excessive in relation to the purposes for which they are processed; and that they shall be preserved in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data are processed.

Given that, within the operational-criminal records, the Controller keeps records and processes data on natural and legal persons for whom there are grounds for suspicion that they have committed criminal offences, as well as data on the outcome of criminal prosecution, for the purpose of clarifying criminal offences, the Commissioner finds that, once the proceedings initiated on the basis of a criminal report have been concluded and the conviction has been expunged, any further processing of such data is contrary to the principles of personal data processing that all controllers must observe. These principles, prescribed in Article 5 of the Law on Personal Data Protection—particularly the principles of purpose limitation, data minimisation, and storage limitation—require cessation of processing once the purpose for which the data were collected and processed has been fulfilled.

The obligation to reassess retention periods and the obligation to erase data when they are no longer necessary for the purposes for which they were collected and used, prescribed in Article 7, paragraph 2 of the Law

on Records and Processing of Data in the Field of Internal Affairs, applies to all records regulated by that Law, including the data contained in the records referred to in Article 41. Although the Law prescribes a specific retention period for each record and stipulates permanent retention for the records under Article 41, the cited provision expressly allows the possibility of erasing data before the expiry of the retention period when the reasons for which the data were entered into a given record no longer exist.

When deciding on a data subject's request for erasure, the Controller must apply both the provisions of the Law on Records and Processing of Data in the Field of Internal Affairs in their entirety and the provisions of the Law on Personal Data Protection as the overarching legal framework governing personal data processing, as well as the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which the Republic of Serbia has ratified. Therefore, for processing to be lawful, compliance with the principle of lawfulness alone is not sufficient; all principles set out in Article 5 of the Law on Personal Data Protection must be met cumulatively, including the principle of storage limitation—which requires that personal data be kept in a form allowing identification only for as long as necessary to achieve the purpose of processing—the principle of data minimisation, and the principle of purpose limitation.

Furthermore, when deciding whether personal data are still necessary for the purpose for which they were collected, the instruments of the Council of Europe were also taken into account, in particular Recommendation R (87) 15 of the Committee of Ministers of the Council of Europe to Member States, which regulates the use of personal data in the police sector. This Recommendation prescribes that measures should be taken to ensure that personal data retained for police purposes are erased if they are no longer necessary for the purpose for which they were stored. In line with this, the following criteria should be specifically considered: the need to retain the data in light of the completion of an investigation; the final judicial decision, especially an acquittal; rehabilitation, served sentences, amnesties; the age of the data subject; special categories of data; as well as the case-law of the European Court of Human Rights (in particular, the judgment in S. and Marper v. the United Kingdom, applications nos. 30562/04 and 30566/04, judgment of 4 December 2008).

Therefore, since the law does not precisely regulate the conditions for the erasure of personal data, and given that the mere retention of data on a person in respect of whom, on the basis of the criminal report KU 131/96 filed against the complainant, criminal proceedings were conducted and lawfully concluded, and the conviction imposed in those proceedings was erased from the criminal records, has a stigmatising effect on that person and jeopardises his constitutional rights – specifically, it calls into question

the legal certainty of the data subject and the equal enjoyment of fundamental human rights, which depends on whether the person's data continue to be processed in the operational-criminalistic database (rights relating to employment, freedom of movement and other rights) – it is necessary that the Controller, in each individual case, assess whether the further processing of certain personal data in the operational-criminalistic database relating to persons for whom, at a given point in time, there existed grounds for suspicion that they had committed a criminal offence, and for whom a criminal complaint had been filed, but where such grounds no longer exist, is necessary for achieving the prescribed purpose of the processing – the clarification of criminal offences.

Having regard to the above, since in the present case the personal data of the complainant are no longer necessary for the purpose for which they were collected, because by the decision of the Municipal Court in Novi Sad, Žabalj Department, the judgment of the Municipal Court in Žabalj, K.113/96, which became final on 24 January 1997, was erased on 10 April 2000, rendered in the criminal proceedings conducted against the complainant on the basis of the criminal report KU 131/96, and more than 25 (twenty-five) years have elapsed since then, and the complainant is considered a person without a criminal conviction, and since the continued retention of such data does not constitute a necessary and proportionate measure in a democratic society, the Commissioner finds that the conditions have been met for the erasure of the complainant's personal data from the Controller's operational-criminalistic database in connection with the aforementioned criminal report, as prescribed by the Law on Personal Data Protection and the Law on Records and Processing of Data in the Field of Interior Affairs.

We point out that even if Article 32 of the Law on Personal Data Protection, which the Controller refers to in its statement, were to be applied, in the present case the conditions for erasure would still be fulfilled, given that further processing is contrary to the purpose-limitation principle, the data-minimisation principle, and the storage-limitation principle under Article 5 of the same law.

Therefore, on the basis of Article 79(2)(7), in connection with Article 77(2) of the Law on Personal Data Protection, and Article 136(1) of the Law on General Administrative Procedure, a decision has been rendered as set out in Sections I, II and IV of the operative part of this decision.

Article 12(1)(3) of the Law on Personal Data Protection prescribes that processing shall be lawful if it is necessary for compliance with the legal obligations of the controller.

Article 30(5) of the Law on Personal Data Protection prescribes that paragraphs 1 to 3 of this Article shall not apply to the extent that the processing is necessary for compliance with a legal obligation of the controller

requiring such processing, or for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

Article 32(1) of the Law on the Prevention of Domestic Violence ("Official Gazette of the RS", nos. 94/2016 and 10/2023 – other law) prescribes that the competent police department shall maintain records on reported cases of domestic violence and on the issuing and enforcement of emergency measures, as well as on the enforcement of protective measures against domestic violence. Paragraph 2 of the same Article prescribes that the records of the police department shall contain: 1) data on reported cases of domestic violence (participants in the event, time, place, collected statements, circumstances of the case, data on the possible victim, etc.); 2) data on the reported possible perpetrator (name, surname, unique citizen identification number, address of permanent or temporary residence, and data on previously imposed protective measures against domestic violence); 3) data on the risk assessment and the names of the authorities to which the risk assessment was submitted; 4) data on the issuing of emergency measures (date and number of the order imposing the emergency measures, their duration and the time when their duration commenced); 5) data on the extension and enforcement of emergency measures (number and date of the decision of the basic court extending the emergency measures, and data on the enforcement of those measures); 6) data on the enforcement of protective measures against domestic violence. Paragraphs 10, 11 and 12 of the same Article prescribe that the records of the police departments, basic courts, basic public prosecutor's offices and social welfare centres shall be kept in electronic form and constitute the Central Register of Cases of Domestic Violence (hereinafter: the Central Register), maintained by the Republic Public Prosecutor's Office; that data may be entered into the Central Register only through the use of appropriate protected access codes; and that the data shall be kept in the records and in the Central Register for ten years and shall thereafter be deleted.

Having regard to the foregoing, and given that the Controller processes the complainant's personal data in the register for the prevention of domestic violence, as well as the fact that Article 32(11) of the Law on the Prevention of Domestic Violence prescribes that data contained in these records and in the Central Register shall be stored for ten years, and bearing in mind that it follows from the Controller's statement and the other submitted evidence that the personal data relating to the complainant were entered into the register for the prevention of domestic violence in 2020, and that the statutory ten-year retention period has not expired, and considering the purpose of the processing, the Commissioner finds that, at this moment, the conditions for erasing the said personal data, as prescribed by the Law on Personal Data Protection and the Law on the Prevention of

Domestic Violence, have not been met, and that the continued processing and storage of these data does not call into question the principles of purpose limitation and storage limitation.

Therefore, pursuant to Article 78(1)(6) of the Law on Personal Data Protection and Article 136(1) of the Law on General Administrative Procedure, the Commissioner has decided as set out in paragraph III of the operative part of this decision.

Case Number: 072-16-4200/2025-06

2.10. The Controller did not respond to the complainant's request in accordance with the Law on Personal Data Protection, but instead invited him to visit the nearest branch office for the purpose of updating his data

From the reasoning:

The Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) received, on 7 November 2024, a complaint, supplemented on 26 November 2024, submitted by AA concerning a violation of the right of access to personal data by Telekom Srbija a.d. Belgrade, as the controller (hereinafter: the Controller). In the complaint, the complainant stated that the user address, i.e. his address, had been altered on the bill for September and the following month of 2024, although the addressee's address had not been changed and remained correct, that is, identical to that in previous bills; that he initially lodged an oral objection with the Controller via telephone, to which no response was provided, following which he sent an e-mail repeating the question from his objection as to how the Controller had obtained his new address, given that he had not provided it. He further stated that the only response he received from the Controller was an instruction to visit the nearest branch office.

Upon reviewing the complaint and the documentation contained in the case file, a decision has been rendered as stated in the operative part of this ruling, for the following reasons:

Article 4 paragraph 1 sub-paragraph 1 of the Law on Personal Data Protection prescribes that personal data is any information relating to a natural person whose identity is determined or determinable, directly or indirectly, particularly based on an identity marker such as name and identification number, location data, identifiers in electronic communications networks, or one or more characteristics of that person's physical, physiological, genetic, mental, economic, cultural or social identity; while subparagraph 2 prescribes that the data subject is a natural person whose personal data are processed.

Article 21 paragraph 1 of the Law on Personal Data Protection prescribes, inter alia, that the controller is obliged to take appropriate measures to provide the data subject with all information relating to the exercise of the rights laid down by this Law, in a concise, transparent, intelligible and easily accessible manner, using clear and plain language. Such information shall be provided in writing or by other means, including in electronic form where appropriate. Paragraph 2 prescribes, inter alia, that the controller is obliged to assist the data subject in exercising his or her rights. Paragraph 3 prescribes, inter alia, that the controller is obliged to provide the data subject with information on action taken on a request without undue delay and at the latest within 30 days of receipt of the request. Paragraph 4 prescribes that, where the controller does not act on the request of the data subject, the controller shall inform that person without delay, and at the latest within 30 days of receipt of the request, of the reasons for not acting, as well as of the right to lodge a complaint with the Commissioner or to bring an action before a court.

Article 79 paragraph 2 item 3 of the same Law prescribes that the Commissioner may order the controller or the processor to act upon the request of the data subject concerning the exercise of their rights, in accordance with this Law.

Having regard to the substance of the request, the controller's responses in the electronic correspondence, the allegations set out in the complaint, as well as the cited legal provisions, the Commissioner finds that the complaint is well-founded, as the controller failed to act upon (i.e. decide on) the request by which the complainant sought the exercise of rights relating to the processing of personal data concerning him, in accordance with the Law on Personal Data Protection. Namely, since it has been established that the complainant, first through an oral objection and subsequently through a request dated 5 November 2024, asked the controller to provide information on the origin of the data concerning his address in … Street, the controller was, pursuant to the cited provision of Article 21 of the Law on Personal Data Protection, obliged to take appropriate measures to provide the data subject with the information relating to the exercise of rights under Article 26 of the Law, or, alternatively, to inform him of the reasons for not acting upon the submitted request, having regard to Article 4 paragraph 1 items 1) and 2) of the Law on Personal Data Protection. As the controller failed to do so in this case, the Commissioner finds that there has been a violation of the complainant's rights relating to the processing of his personal data.

The Commissioner considered the controller's statements in its responses to the complainant dated 10 October 2024 and 6 November 2024, but these could not influence a different decision, given that the controller did not reply to the complainant's request of 5 November 2024 in accordance

with Article 21 of the Law on Personal Data Protection, but instead invited him to visit the nearest branch office for the purpose of updating his data.

Therefore, without deciding on the merits of the request, the Commissioner, pursuant to Article 79 paragraph 2 item 3, in conjunction with Article 77 paragraph 2 of the Law on Personal Data Protection, and Article 136 paragraph 1 of the Law on General Administrative Procedure, has decided as set out in items I and II of the operative part of this decision.

Case Number: 072-16-2584/2024-06

2.11. The complainant is exercising a right contrary to the purpose for which it was established

From the reasoning:

The Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) received, on 25 April 2025, a complaint submitted by AA concerning a violation of the right of access to personal data by the Centre for Social Work "Trstenik" in Trstenik, as the data controller (hereinafter: the Controller), in relation to the request for exercising rights regarding the processing of personal data dated 3 March 2025. In the complaint, he stated that the Controller had not fully acted upon his request, as it had failed to inform him about question No. 3, namely in what capacity he had been recorded in the Controller's records (as a perpetrator of violence, a victim, or something else). He further stated that no report had ever been filed against him and that he had a "legal interest in challenging unlawful actions carried out against him without legal grounds".

In its response to the complaint dated 7 May 2025, the Controller stated that the complaint was unfounded, because it had already responded to the identical question in its letter No. … of 21 June 2023, informing him that the Basic Court in Trstenik, by judgment No. … of 7 December 2021, had imposed protection measures against domestic violence, and that he had been recorded in the active domestic violence register as a person against whom such measures had been imposed and as a person to whom protection measures against domestic violence applied. The Controller added that persons in this register are not labelled as perpetrators of violence, nor is the complainant labelled as such, and that the complainant, being dissatisfied with the response, is repeating the same request. It also stated that the case concerning the family … had been closed on 21 July 2023, as no new reports of domestic violence had been filed since 18 November 2022, and that the protection measures had expired on 31 March 2023.

Upon examining the complaint, a decision has been adopted as set out in the operative part of this ruling, for the following reasons:

Pursuant to Article 4 of the Rulebook on the Records and Documentation Concerning Persons Against Whom Domestic Violence Has Been Committed and Persons Against Whom a Protection Measure Against Domestic Violence Has Been Ordered ("Official Gazette of the RS", No. 88/23), it is prescribed, inter alia, that the records concerning persons against whom domestic violence has been committed and persons against whom a protection measure has been ordered shall contain the data from the judgment by which the protection measures against domestic violence have been imposed.

Under Article 26 paragraph 1 of the Law on Personal Data Protection, the data subject has the right to request from the controller information as to whether his or her personal data are being processed, access to those data, as well as the following information: 1) the purpose of processing; 2) the types of personal data being processed; 3) the recipient or categories of recipients to whom the personal data have been disclosed, in particular recipients in other states or international organisations; 4) the envisaged period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period; 5) the existence of the right to request from the controller the rectification or erasure of personal data, or the right to request restriction of processing of those data; 6) the right to lodge a complaint with the Commissioner; 7) available information on the source of the personal data if the personal data have not been collected from the data subject; 8) the existence of automated decision-making, including profiling referred to in Article 38 paragraphs 1 and 4 of this Law. Pursuant to paragraph 3 of the same Article, the controller is obliged, at the request of the data subject, to provide a copy of the personal data undergoing processing.

Taking into account the established facts and the cited legal provisions, the Commissioner finds that the complaint is unfounded. This is because the content of the request indicates that, in the present case, it does not concern a request for exercising the right of access to personal data on the basis of which a data subject is entitled to request information, including the type of data processed by the Controller in accordance with the aforementioned Article, but rather that the complainant is using this right contrary to the purpose for which it was established, namely, to be informed of the data which the Controller processes about him within the records it keeps in accordance with the cited provision of Article 4 of the Rulebook on the Records and Documentation Concerning Persons Against Whom Domestic Violence Has Been Committed and Persons Against Whom a Protection Measure Against Domestic Violence Has Been Ordered.

Furthermore, the Controller has submitted evidence that it had already informed the complainant of the above by letter No. 03-560-762/1 of 21 June 2023, which the complainant does not dispute.

Accordingly, on the basis of Article 78 paragraph 1 item 6, in conjunction with Article 77 paragraph 2 of the Law on Personal Data Protection and Article 136 paragraph 1 of the Law on General Administrative Procedure, it has been decided as set out in the operative part of this ruling.

Case Number: 072-16-3164/2025-06

2.12. Binding Corporate Rules

From the reasoning:

On 9 May 2025, the company "ACUMATICA" d.o.o. Belgrade submitted to the Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) a request for the approval of Binding Corporate Rules.

The applicant enclosed, along with the request, the Binding Corporate Rules for which approval is sought.

Upon examining the request and the remaining case file, a decision has been rendered as set out in the operative part of this ruling, for the following reasons:

Article 4, point 21) of the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18) stipulates that binding corporate rules are internal personal data protection rules adopted and applied by a controller or processor with a domicile, residence or registered seat in the territory of the Republic of Serbia, for the purpose of regulating the transfer of personal data to a controller or processor in one or more countries within a multinational company or group of undertakings.

Articles 65(1) and (2) of the aforementioned Law stipulate that a controller or processor may transfer personal data to another country, to a part of its territory, or to one or more sectors of specific activities within that country, or to an international organisation for which the list referred to in Article 64(7) of this Law has not established the existence of an adequate level of protection, only if the controller or processor has ensured appropriate safeguards for such data and if the data subject is guaranteed the exercise of his or her rights and effective legal protection. The provision further prescribes that appropriate safeguards may be ensured without the Commissioner's specific approval, inter alia, by means of Binding Corporate Rules, in accordance with Article 67 of this Law.

Article 67 of the same Law prescribes that the Commissioner shall approve Binding Corporate Rules if those rules, taken together, fulfil the following conditions:

1) they are legally binding, apply to and are implemented by every member of the multinational company or group of undertakings, including their employees;

2) they expressly ensure the exercise of the rights of data subjects in relation to the processing of their data;
3) they meet the requirements laid down in paragraph 2 of this Article.

Binding Corporate Rules referred to in paragraph 1 of this Article must, at a minimum, determine the following:

1) the structure and contact details of the multinational company or group of undertakings, as well as of each of its members;
2) the transfer or group of transfers of personal data, including the types of personal data, the types of processing operations and their purpose, the categories of data subjects, and the name of the country to which the data are transferred;
3) the mandatory nature of the application of the Binding Corporate Rules, both within the multinational company or group of undertakings and outside them;
4) the application of the general principles of personal data protection, particularly purpose limitation, data minimisation, storage limitation, data integrity, measures for continuous data protection, the legal basis for processing, the processing of special categories of personal data, security measures, and the conditions for any further transfers of personal data to bodies or recipients not bound by the Binding Corporate Rules;
5) the rights of data subjects in relation to the processing and the manner in which those rights may be exercised, including rights relating to automated individual decision-making and profiling under Article 38 of this Law, the right to lodge a complaint with the Commissioner or to bring an action before a court in accordance with Articles 82 and 84 of this Law, as well as the right to compensation for damage arising from a breach of the Binding Corporate Rules;
6) the acceptance of liability by the controller or processor with residence, domicile, or registered seat in the territory of the Republic of Serbia, for a breach of these rules committed by another member of the group which does not have residence, domicile, or registered seat in the territory of the Republic of Serbia, unless the controller or processor proves that such member of the group is not responsible for the event which caused the damage.
7) the manner in which information on the Binding Corporate Rules is provided to the data subject, particularly the provisions referred to in items 4) to 6) of this paragraph, together with the provision of other information referred to in Articles 23 and 24 of this Law;
8) the powers of the data protection officer appointed in accordance with Article 58 of this Law, or of any other person authorised to supervise the application of the Binding Corporate Rules within the multinational company or group of undertakings, including supervision

of training and decision-making on complaints within the multinational company or group;

9) the procedure applied in relation to complaints;
10) the mechanism for verifying compliance with the Binding Corporate Rules within the multinational company or group of undertakings. This mechanism shall include a personal data protection audit and corrective measures for safeguarding the rights of data subjects. The results of the verification must be communicated to the person referred to in item 8) of this paragraph, as well as to the management body of the multinational company or group of undertakings, and must also be made available to the Commissioner upon request;
11) the method of reporting and keeping records on amendments to the Binding Corporate Rules and the method of notifying the Commissioner of those amendments;
12) the manner of cooperation with the Commissioner with a view to ensuring the application of the Binding Corporate Rules by each individual member of the multinational company or group of undertakings, particularly the manner in which the results of the verification referred to in item 10) of this paragraph are made available to the Commissioner;
13) the manner of reporting to the Commissioner on legal obligations applicable to a member of the multinational company or group of undertakings in another country, which may have a significantly adverse impact on the safeguards prescribed by the Binding Corporate Rules.
14) appropriate personal data protection training for persons who have permanent or regular access to personal data.

The Commissioner may further regulate the manner of exchange of information between controllers, processors and the Commissioner in the application of paragraph 2 of this Article.

If the conditions referred to in paragraph 1 of this Article have been met, the Commissioner shall approve the Binding Corporate Rules within 60 days from the date of submission of the request for their approval.

Following an examination of the Binding Corporate Rules submitted by the applicant, the Commissioner established that they apply to all personal data processed in the Republic of Serbia by members of the group, i.e. companies operating within the ACUMATICA group, when acting as controllers or internal processors, and which are transferred from a group member established in the Republic of Serbia to group members established outside the territory of the Republic of Serbia.

The Binding Corporate Rules apply to personal data of job applicants, i.e. natural persons applying for employment or professional development (internships) with the members of the group. In such cases, the data may be disclosed or transferred to any member of the group that has a legitimate interest relating to the candidate's application, which may result in an international transfer of data. The Rules also apply to personal data of employees of the companies that are members of the group, collected on the basis of the employment relationship, during its establishment and throughout its duration.

An examination of Annex 1 to the Binding Corporate Rules established that the members of the group are companies headquartered in the United States of America, Canada, the United Kingdom and Sri Lanka.

Following a review of the content of the aforementioned documents, the Commissioner established that they are legally binding on all companies operating within the ACUMATICA group, including their employees; that they expressly ensure the rights of employees and the company's business partners in situations where their data are processed and transferred; that they prescribe the structure and contact details of the group members; that they identify the types of data processed and transferred; that they prescribe the application of the general principles of personal data protection; that they determine the rights of data subjects in relation to the processing and the methods of exercising those rights; that they provide for the liability of the company "ACUMATICA" d.o.o. Beograd for any breach of the Binding Corporate Rules committed by any other group member not established in the Republic of Serbia; that they define the manner in which data subjects are provided with information on the Binding Corporate Rules; that they set out the procedure to be followed in the event of complaints; that they prescribe the method of cooperation with the Commissioner and reporting to the Commissioner; and that they contain other provisions fulfilling the requirements set out in Article 67, paragraph 2 of the Law on Personal Data Protection.

In view of the above, the Commissioner found that the Binding Corporate Rules of 5 May 2025 submitted by the applicant meet the conditions laid down in Article 67, paragraph 1 of the Law on Personal Data Protection and ensure appropriate safeguards for personal data. Consequently, the conditions for their approval have been fulfilled, and therefore, on the basis of Article 67, paragraphs 1 and 4, Article 78, paragraph 1, item 20) and Article 79, paragraph 3, item 8) of the said Law, a decision was rendered as set out in the operative part of this ruling.

Case Number: 072-18-3210/2025-06

2.13. The action taken by an authority in response to a request that is identical or similar in content to a request by which a person seeks to exercise rights relating to the processing of personal data concerning that person cannot be regarded as action taken in two separate administrative matters

From the reasoning:

The Commissioner for Information of Public Importance and Personal Data Protection (hereinafter: the Commissioner) received, on 15 October 2025, a complaint submitted by AA due to a violation of the right of access to personal data by the Joint Stock Company "Elektroprivreda Srbije" of Belgrade, as the data controller (hereinafter: the Controller), concerning her request for the exercise of rights related to the processing of personal data dated 1 September 2025. In the complaint, she stated that on 14 October 2025 she had received an incomplete response from the Controller regarding her request, from which it follows that the Controller was avoiding providing her with the data it processes about her, and which are contained in the documentation specified in her request. She further stated that the Controller considers that it already provided her with employment-related documentation in June 2025, but that this documentation actually relates to her other requests, and not to the documents she sought through her request of 1 September 2025 submitted pursuant to the Law on Personal Data Protection, since the Controller had not, inter alia, provided her with the decision on unpaid leave or the documentation relating to the disciplinary procedure conducted against her.

In its statement on the complaint of 13 November 2025, the Controller fully upheld the assertions made in its response of 14 October 2025 and added that the complainant's request was not aimed at exercising rights relating to the processing of personal data, even though it was submitted with reference to the provisions of the Law on Personal Data Protection, but that its purpose was the delivery of specifically enumerated documents. It further stated that it considers that no violation of rights to her detriment had occurred, as the complainant has not been employed since 17 September 2020, and therefore her personal data are no longer processed on the basis of employment, but only retained as documentation arising from such employment, in accordance with the law. The Controller also stated that it had already provided the complainant with the available employment-related documentation, both during and after the termination of her employment, as well as through the judicial proceedings initiated by the complainant and pending before the Higher Court in Novi Sad and the First Basic Court in Belgrade.

Having examined the complaint, a decision was rendered as stated in the operative part of this ruling for the following reasons:

Pursuant to Article 4, paragraph 1, item 1) of the Law on Personal Data Protection, it is prescribed, inter alia, that personal data are any data relating to a natural person whose identity is determined or determinable, directly or indirectly; item 2) prescribes that the data subject is a natural person whose personal data are processed; and item 3) prescribes that the processing of personal data means any operation or set of operations performed, whether automated or non-automated, on personal data or sets of personal data, such as collection, recording, sorting, grouping or structuring, storage, adaptation or alteration, disclosure, access, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, comparison, restriction, erasure or destruction.

Pursuant to Article 21, paragraph 1 of the Law on Personal Data Protection, it is prescribed, inter alia, that the controller is obliged to take appropriate measures in order to provide the data subject with all information relating to the exercise of the rights laid down by this law, in a concise, transparent, intelligible and easily accessible manner, using clear and plain language. Such information shall be provided in writing or in another form, including electronic form where appropriate. Paragraph 2 prescribes, inter alia, that the controller is obliged to assist the data subject in the exercise of his or her rights. Paragraph 3 prescribes, inter alia, that the controller is obliged to provide the data subject with information on action taken on the request without delay, and at the latest within 30 days of receipt of the request. Paragraph 4 prescribes that, where the controller does not act on the request of the data subject, the controller shall inform that person without delay, and at the latest within 30 days of receipt of the request, of the reasons for not acting, as well as of the right to lodge a complaint with the Commissioner or to initiate court proceedings.

Pursuant to Article 26, paragraph 1 of the Law on Personal Data Protection, it is prescribed, inter alia, that the data subject has the right to request from the controller information as to whether his or her personal data are being processed, access to such data, as well as the following information: the purpose of the processing; the types of personal data being processed; the recipient or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in other states or international organisations; the envisaged period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period; the existence of the right to request from the controller the rectification or erasure of his or her personal data; the right to lodge a complaint with the Commissioner; available information on the source of the personal data if the personal data have not been collected from the data subject; and the existence of automated decision-making, including profiling referred to in Article 38, paragraphs 1 and 4 of this Law, and, at least in such cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Pursuant to Article 79, paragraph 2, item 3 of the same Law, it is prescribed that the Commissioner may order the controller or processor to act upon the request of the data subject concerning the exercise of his or her rights, in accordance with this Law.

Having regard to the fact that the Controller did not act upon the Complainant's request and did not, within the 30-day time limit, provide her with all information relating to the exercise of the right prescribed by this Law, nor provide her with the information and copies of the data concerning her, insofar as the requested information were in its possession, nor, indeed, inform the Complainant of the reasons for failing to act upon the said request, the Commissioner finds that the complaint is well-founded. In doing so, the Commissioner did not assess the merits of the request from the perspective of any right by which the Complainant sought access to data relating to third parties. Namely, pursuant to the cited provision of Article 21 of the Law on Personal Data Protection, the Controller is obliged to take appropriate measures in order to provide the data subject with information relating to the exercise of the right referred to in Article 26 of this Law or, alternatively, to inform the applicant of the reasons for not acting upon the request, bearing in mind the provisions of Article 4, paragraph 1, items 1), 2) and 3) of the Law on Personal Data Protection. As the Controller, in this particular case, failed to do so and did not act upon the request for the exercise of rights, the Commissioner finds that a violation of the Complainant's rights concerning the processing of personal data has occurred.

The Controller's assertion that the requested documentation was delivered to the Complainant on 11 June 2025 has been taken into consideration but could not be upheld and could not influence a different decision on the complaint. This is because the actions taken by an authority upon a request that is identical or similar in content to a request by which an individual seeks to exercise rights related to the processing of personal data concerning that individual cannot be regarded as action taken in both administrative matters. Namely, the Controller is obliged to act upon a request submitted pursuant to the Law on Personal Data Protection, which, in this specific case, it failed to do. Furthermore, the Controller did not submit evidence showing that the same documentation requested under the application for the exercise of rights concerning the processing of personal data of 1 September 2025 had already been provided to the Complainant on 11 June 2025.

Therefore, without deciding on the merits of the request, and on the basis of Article 79(2)(3), in connection with Article 77(2) of the Law on Personal Data Protection, and Article 136(1) of the Law on General Administrative Procedure, the Commissioner has ruled as set out in the operative part of this decision.

Case Number: 072-16-4618/2025-06

3. QUESTIONS AND ANSWERS

The Commissioner for Information of Public Importance and Personal Data Protection is contacted on a daily basis by a large number of citizens, legal entities, associations, as well as public authorities, with questions and uncertainties regarding the application of the LPDP.

Below, we have highlighted those questions that were most relevant in the previous year.

3.1. Registration on the public authority's website and processing of personal data

Question: The opinion was requested in connection with the planned launch of a new public authority website "which provides an optional possibility for citizens to register on the said website", stating that registration of a user account is not mandatory and does not represent any prerequisite for accessing the content of the site… that the registration is used for the purpose of collecting users' e-mail addresses and obtaining users' consent to receive promotional notifications from the authority relating to the current and new services the authority provides to citizens; that the registration enables users "to manage their consents regarding the receipt of such notifications at any time"; and that the registration "requires only the entry of an e-mail address", and that the user "does not submit any personal data".

An e-mail address, if it is structured in such a way that a person's identity can be determined from it either directly or indirectly, in combination with other information, certainly constitutes personal data. In addition, a login or, as stated, "registration" of a user account often contains, alongside the e-mail address, other personal data. The processing of personal data is any operation or set of operations performed, whether automated or non-automated, on personal data or sets of personal data, such as collection, recording, sorting, grouping or structuring, storage, adaptation or alteration, disclosure, access, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, comparison, restriction, erasure or destruction.

First, we note that your submission does not make clear what is meant by the term "registration of citizens", what the purpose of such "registration" is, within which technological system this "registration" would be carried out and in what manner it would be introduced, who would have access to it, nor what you mean by "obtaining users' consent", and whether this refers to consent for the processing of personal data, which types of personal data, for which specific purpose, which category of individuals is concerned, and all other relevant aspects that are important for determining whether the conditions for the lawfulness of a given processing activity are met.

Therefore, we hereby generally point out the following:

It should first be borne in mind that the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18) regulates, in a systemic manner, the principles of personal data processing, as well as other general rules and obligations of controllers and other entities processing personal data, whereas the processing of personal data in specific areas of social

life/activities is regulated by special regulations whose implementation is overseen by other authorities.

Pursuant to Article 4, point 1 of the Law, personal data is any information relating to an identified or identifiable natural person, directly or indirectly, particularly on the basis of an identifier such as a name or identification number, location data, an identifier in electronic communication networks, or one or more characteristics of that person's physical, physiological, genetic, mental, economic, cultural or social identity.

We note that the Law prescribes conditions that must be met for the lawfulness of any processing of personal data.

Namely, every controller is obliged to comply with the principles of processing prescribed by this Law, specifically the principles of "lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation" and "integrity and confidentiality" (Article 5, paragraph 1 of the Law).

Furthermore, an appropriate legal basis must be ensured for every processing of personal data, i.e. all personal data processing must be lawful in accordance with Article 12, points 1–6 of the Law. When it comes to personal data processing carried out by controllers for the purpose of complying with the controller's legal obligations, or for processing that is necessary for performing tasks carried out in the public interest or for exercising powers vested in the controller by law, within the meaning of Article 12, paragraph 1, points 3 and 5 of the Law, the basis for such processing is established by law. Accordingly, the legal basis for the processing of personal data carried out by a public authority in the performance of its duties and powers must derive from the relevant special laws.

Therefore, for certain personal data processing to be permissible from the standpoint of the application of the Law, it is necessary that the purpose of processing first be specifically defined, explicit, justified and lawful; that there be an appropriate legal basis for the intended processing in accordance with Article 12, taking into account the special regulations governing processing in the specific case; and that the processing be carried out in line with the processing principles set out in Article 5 of this Law, in particular the principle of "data minimisation."

In each specific case, the controller must ensure that it collects only those data that are adequate, relevant and limited to what is necessary in relation to the purpose of the processing. The data to be processed must be reduced to the minimum necessary to achieve the purpose of the processing; in other words, any data without which the purpose of the processing could still be fulfilled would constitute superfluous data and, as such, processing that is contrary to the aforementioned principle.

The controller is also responsible for fulfilling other obligations established by the Law, such as: providing information on the processing (Article 23), taking appropriate measures to protect personal data (Articles 41 and 42 of the Law), the obligation to keep records of processing activities (Article 47 of the Law), and others. Proper fulfilment of these obligations must be assessed in each individual case, depending on all relevant facts and circumstances (taking into account the nature, scope and purpose of the processing, as well as the special regulations governing the particular area, etc.).

In this regard, we remind you that a controller who has appointed a data protection officer is required to involve that person in a timely and appropriate manner in all activities related to the protection of personal data, in accordance with Article 57, paragraph 1 of the Law, including informing and providing opinions to the controller, as well as to employees who carry out processing activities, regarding their statutory obligations in relation to personal data protection.

Pursuant to Article 5, paragraph 2 of the Law, responsibility for compliance lies with the controller, who must be able to demonstrate that the intended processing is in accordance with the Law.

Therefore, before any intended processing is commenced — which must be lawful and based on an appropriate legal ground arising from the special regulations governing the subject matter — it is first necessary to determine the purpose of such processing in a clear, specific and explicit manner; then to assess whether the intended processing is justified, that is, whether it is necessary for achieving that purpose and proportionate to it, or whether the purpose can be achieved without such processing, taking into account, for example, the type and scope of personal data to be processed, the categories of individuals whose data would be processed, and other relevant factors.

Case Number: 073-14-5688/2024-02

3.2. Are hunting associations required to appoint a data protection officer?

Question: The opinion was requested regarding whether hunting associations fall within the categories that, under the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018), are required to appoint a data protection officer. In its submission, the applicant states that, in their view, hunting associations do not fall within the categories of controllers or processors obliged to appoint a data protection officer because "they are not public authorities—they are established by their members, their funds

come from membership fees, and they are not financed by the state", while some associations "receive certain funds on the basis of competing for incentive funding for their regular activities". It is further stated that the core activities of hunting associations "are not processing operations which, by their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale"; that hunting associations "undoubtedly process the personal data of their members in the course of issuing hunting permits…", and that hunting associations do not process special categories of personal data referred to in Article 17, paragraph 1, nor data relating to criminal convictions and offences referred to in Article 19 of the Law.

The Commissioner is of the opinion that hunting associations and other associations that exercise public powers in accordance with the Law on Game and Hunting, such as the powers granted within the right to manage a hunting ground, have the status of public authorities under the Law on Personal Data Protection and, consequently, are obliged to appoint a data protection officer. We also draw attention to Article 56, paragraph 6 of the Law on Personal Data Protection, which provides the possibility of appointing a joint data protection officer where the controllers/processors are public authorities, taking into account the organisational structure and size of those authorities.

When it comes to the obligation to appoint a data protection officer, this obligation is established in the cases prescribed by Article 56, paragraph 2 of the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018). Accordingly, a controller or processor is required to appoint a data protection officer if:

1) the processing is carried out by a public authority, except where the processing is performed by a court for the purpose of exercising its judicial powers;
2) the core activities of the controller or processor consist of processing operations which, by their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale;
3) the core activities of the controller or processor consist of the large-scale processing of special categories of personal data referred to in Article 17, paragraph 1, or of personal data relating to criminal convictions and offences referred to in Article 19 of this Law.

Having regard to your statements, we would first like to clarify what is understood by the term public authority, since all entities that have the status of a public authority are obliged to appoint a data protection officer, publish that officer's contact details, and submit those details to the Commissioner, who maintains a register of data protection officers, pursuant to Article 56, paragraph 11 of the Law.

In accordance with Article 4, point 25 of the Law, the term public authority refers to: a state authority, an authority of territorial autonomy or a local self-government unit, a public enterprise, an institution or other public service, an organisation, and any other legal or natural person exercising public powers.

In this respect, the special regulations in the relevant field must be taken into account as a priority. Matters relating to the protection, management, hunting, use and improvement of game populations within a hunting ground, as well as other issues of importance for game and hunting, are regulated by the Law on Game and Hunting and other special regulations in this area.

Article 38 of that Law regulates the granting of the right to manage a hunting ground. Pursuant to paragraph 1 of that Article, the right to manage a hunting ground may be acquired by a single hunting ground user who meets the conditions prescribed by the Law. Paragraph 3 of the same Article stipulates that a hunting ground user may be a legal person established as a public enterprise, a commercial company, another form of enterprise, as well as hunting associations and other associations established and operating in accordance with the law. The Law on Game and Hunting also prescribes the duties of hunting ground users, such as issuing hunting permits in the prescribed form, keeping prescribed records, and similar tasks.

Case Number: 073-14-5436/2024-02

3.3. Possibility of installing "People Counter" technology in retail facilities

Question: A commercial company plans to install People Counter devices in retail facilities, consisting of "a camera positioned towards the entrance of the retail facility, producing a real-time image for the purpose of counting persons entering and exiting the retail space", whereby, as stated, no footage is stored and "the People Counter would be used exclusively for marketing purposes". In this regard, the question posed to this authority is whether this constitutes processing of the data of individuals entering the facility, and "whether any documentation is required for compliance with the regulations, given that this does not constitute video surveillance."

The Commissioner is of the opinion that, when deciding how to act in specific situations—particularly when introducing new technological solutions—the controller must first determine whether the situation involves the processing of personal data within the meaning of the Law. If

the controller concludes that personal data would be processed, it must assess whether the purpose of the processing could be achieved in another manner that is less intrusive to privacy and/or other fundamental rights and freedoms of individuals, taking into account the type of personal data (including whether special categories of data, such as biometric data within the meaning of Article 17 of the Law, are processed). Before any processing is commenced, the controller must determine whether all conditions required for lawful processing under the Law are fulfilled. The purpose of the processing must first be specifically defined, explicit, lawful and justified, and the processing must be genuinely necessary for achieving that purpose—that is, whether the controller truly requires such processing. An adequate legal basis must be ensured for the processing, and the processing must be carried out in accordance with special regulations governing the relevant field/activity, while respecting the aforementioned processing principles and other obligations established by the Law.

In this regard, we provide the following information.

First, we note that the purpose of introducing the specified technology is not clear, nor the manner in which it would be used, whether it would involve the processing of personal data, nor consequently any of the aspects of personal data processing that would be carried out in that context.

The Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018) does not contain specific provisions on video surveillance, while the Law on Private Security ("Official Gazette of the RS", Nos. 104/2013, 42/2015 and 87/2018) regulates the mandatory security and protection of certain facilities, the activities and operations of legal and natural persons in the field of private security, the conditions for their licensing, the manner of performing such activities, and the exercise of supervision over their work. Since, pursuant to Article 70 of the Law on Private Security, supervision over the application of that law is exercised by the Ministry of the Interior, we point out that you may contact that Ministry in order to obtain an opinion regarding the application of the provisions of that law.

Under the Law on Personal Data Protection, the application of which is overseen by the Commissioner, the principles of personal data processing are regulated in a systemic manner, together with other general rules and certain obligations for controllers and other subjects, while the processing of personal data in specific sectors/activities is regulated by special regulations.

Therefore, we would first like to clarify the meaning of certain terms defined in the Law on Personal Data Protection.

Personal data, pursuant to Article 4, point 1 of the Law on Personal Data Protection, is any information relating to a natural person whose identity is determined or identifiable, directly or indirectly, particularly on the basis of an identifier such as a name or identification number, location data, an identifier in electronic communications networks, or one or more characteristics of that person's physical, physiological, genetic, mental, economic, cultural or social identity. Furthermore, processing of personal data, pursuant to Article 4, point 3 of the Law on Personal Data Protection, is any operation or set of operations performed, whether by automated or non-automated means, on personal data or sets of personal data, such as collection, recording, sorting, grouping or structuring, storage, adaptation or alteration, disclosure, access, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, comparison, restriction, erasure or destruction.

If, in the specific case, personal data were to be processed within the meaning of Article 4, point 3 of the Law on Personal Data Protection, it must be borne in mind that the Law prescribes the conditions that must be fulfilled for any processing of personal data to be lawful.

Namely, by initiating processing, the controller assumes specific obligations arising from the Law on Personal Data Protection, primarily the obligation to comply with the processing principles set out in Article 5 of the Law, namely the principles of "lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation" and "integrity and confidentiality".

Furthermore, every processing of personal data must have an appropriate legal basis, meaning that all processing must be lawful. Article 12 of the Law on Personal Data Protection prescribes that processing is lawful only if one of the following conditions is met: 1) the data subject has consented to the processing of their personal data for one or more specifically defined purposes; 2) the processing is necessary for the performance of a contract concluded with the data subject or to take steps, at the request of the data subject, prior to entering into a contract; 3) the processing is necessary to comply with the controller's legal obligations; 4) the processing is necessary to protect the vital interests of the data subject or another natural person; 5) the processing is necessary for performing tasks carried out in the public interest or in the exercise of powers vested in the controller by law; 6) the processing is necessary for the purposes of the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data, particularly where the data subject is a minor.

In addition, the controller must comply with other obligations under the Law on Personal Data Protection, such as: taking measures to protect

personal data (Articles 41 and 42), keeping records of processing activities (Article 47), and others.

In this regard, we note that Article 54, paragraph 1 of the Law on Personal Data Protection establishes the controller's obligation to carry out a data protection impact assessment if it is likely that a type of processing, particularly when new technologies are used and taking into account the nature, scope, context and purposes of the processing, will result in a high risk to the rights and freedoms of natural persons, before beginning the processing.

The cases in which the controller is required to conduct a data protection impact assessment are prescribed by Article 54, paragraph 4 of the Law and by the Decision on the List of Types of Personal Data Processing Activities Requiring a Data Protection Impact Assessment and Prior Consultation with the Commissioner ("Official Gazette of the RS", Nos. 45/19 and 112/20).

Since, under the principle of "accountability" set out in Article 5, paragraph 2 of the Law on Personal Data Protection, the controller bears responsibility for the correct application of the Law, this also includes determining whether, in the specific case, personal data processing takes place within the meaning of the Law.

Case Number: 073-14-5239/2024-02.

3.4. Must a processor present the controller in advance with a list of sub-processors (if it intends to engage them), and must the specific country in which the processing will take place be indicated?

Question: The bank has requested an opinion, stating that, as a controller, it is in the process of concluding an agreement with a client acting as a processor to whom it entrusts the performance of certain activities. "The company in question is established in Serbia and is part of a large global company which has a worldwide network of branches registered as separate legal entities, as is the case here… In this case, a Personal Data Processing Agreement will not be concluded in accordance with the Commissioner's Standard Contractual Clauses, but a separate agreement will be drawn up as part of the main contract, which should contain all elements required under the Law on Personal Data Protection."

In this regard, the following questions have been raised: "1. Whether our Client, as the Processor, within the meaning of Article 45 of the Law on Personal Data Protection, must present the Bank in advance with a list of

sub-processors if it wishes to engage sub-processors… and whether, in the data processing agreement, the client may state that the sub-processors may be all companies affiliated with the parent company / belonging to the same Group or representing branches of the parent company, including the parent company itself, and similar; 2. Whether the Processor may engage Sub-processors solely for the specific personal data processing for which it has been engaged by the Controller, and for which the purpose and manner of processing have been determined by the Controller… and whether the Processor may disclose the Controller's employees' personal data to other sub-processors (where the sub-processors, in line with question 1, would be other branches or members of the same Group registered in other countries) for a different purpose, such as, for example, for the purposes of an internal audit carried out by that other company/sub-processor; 3. In relation to the above questions, must the exact country in which the processing or sub-processing will take place be specified? May it instead be stated only that the processing will take place on the territory of the EU, or must a specific country be explicitly indicated (as suggested in Annex 6 to the Commissioner's Standard Contractual Clauses)?"

In this regard, we provide the following information:

A processor may not carry out processing for its own purposes, and it will be deemed to have exceeded its authorisation if it acts outside the controller's instructions and/or if it begins to determine its own purposes and means of processing. A processor may entrust processing to another processor only if the controller authorises it to do so on the basis of a general or specific written authorisation. If the processing is carried out on the basis of a general authorisation, the processor is obliged to inform the controller of any intended engagement or replacement of another processor, so that the controller has the opportunity to object to such a change (Article 45, paragraph 2 of the Law on Personal Data Protection). From the above, it follows that the processor is required to obtain the controller's consent or authorisation before entrusting any personal data processing to any specific sub-processor.

When a controller intends to carry out the processing of personal data, it must, before initiating such processing, ensure that it is conducted in accordance with the relevant special regulations. In the case of processing employees' personal data, pursuant to Article 91 of the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018 – hereinafter: the Law), the employer's authorisation as controller for the intended processing must primarily derive from the relevant regulations in the field of labour, employment, etc., while also applying the principles and complying with the obligations and processing rules prescribed by the Law. This

includes providing information to the data subject in accordance with Article 23 of the Law, as well as taking appropriate protection measures to ensure that the processing is carried out in accordance with the Law and that the controller is capable of demonstrating such compliance, taking into account the nature, scope, context and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons.

From the standpoint of personal data protection, when several different entities participate in a processing operation, it is first necessary to determine the role of each entity so that the provisions of the Law may be correctly applied and all corresponding obligations fulfilled.

A controller is a natural or legal person, or a public authority, which alone or jointly with others determines the purpose and means of processing, while a law that determines the purpose and means of processing may also designate the controller or prescribe the conditions for its designation. A processor, on the other hand, is a natural or legal person, or a public authority, which processes personal data on behalf of the controller. The processor therefore does not determine either the purpose or the means of the processing, meaning that the controller has overall control over the processing. The processor is a separate entity from the controller, performing processing on behalf of (and for the benefit of) the controller, and is typically an organisation or other entity with specific skills and expertise that the controller engages to carry out certain personal data processing activities in its name.

Furthermore, pursuant to Article 45, paragraph 1 of the Law, where processing is carried out on behalf of the controller, the controller may appoint as processor only such a person or public authority that provides full guarantees regarding the application of appropriate technical, organisational and staffing measures, in a manner that ensures that the processing is performed in accordance with the provisions of this Law and that the rights of the data subjects are protected.

Processing by a processor must be governed by a contract or other legally binding act concluded or adopted in written form, including electronic form, which binds the processor to the controller and regulates the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, as well as the controller's rights and obligations (Article 45, paragraph 3 of the Law).

Under the contract or other legally binding act referred to in Article 45, paragraph 3 of the Law on Personal Data Protection, it must be prescribed that the processor is obliged to: 1) process personal data only on the basis of the controller's written instructions, including the instruction relating to the transfer of personal data to other countries or international

organisations, unless the processor is required by law to process the data. In that case, the processor must inform the controller of that legal obligation before commencing the processing, unless the law prohibits providing such information for reasons of protecting an important public interest; 2) ensure that any natural person authorised to process personal data has undertaken an obligation of confidentiality or is subject to a statutory confidentiality obligation; 3) take all necessary measures in accordance with Article 50 of this Law; 4) comply with the conditions for entrusting processing to another processor as set out in paragraphs 2 and 7 of this Article; 5) taking into account the nature of the processing, assist the controller, as far as possible, by applying appropriate technical, organisational and staffing measures, in fulfilling the controller's obligations regarding requests for the exercise of data subjects' rights under Chapter III of this Law; 6) assist the controller in fulfilling its obligations under Article 50 and Articles 52 to 55 of this Law, taking into account the nature of the processing and the information available to the processor; 7) upon completion of the contracted processing activities, and in accordance with the controller's decision, delete or return all personal data to the controller and delete all copies of such data, unless a legal obligation requires their retention; 8) make available to the controller all information necessary to demonstrate compliance with the processor's obligations under this Article, as well as information that enables and contributes to audits or inspections conducted by the controller or by another party authorised by the controller.

If the processor appoints another processor to perform specific processing activities on behalf of the controller, the same personal data protection obligations prescribed in the contract or other legally binding act between the controller and the processor, as referred to in paragraphs 3 and 4 of Article 45 of the Law, shall also bind that other processor. This must be ensured on the basis of a separate contract or other legally binding act concluded or adopted in written form, including electronic form, which, in the relationship between the processor and the additional processor, provides sufficient guarantees regarding the application of appropriate technical, organisational and staffing measures to ensure that the processing is carried out in accordance with the Law. If the additional processor fails to fulfil its obligations concerning personal data protection, the processor remains liable to the controller for the fulfilment of those obligations by the additional processor (Article 45, paragraph 7 of the Law).

We also note that if personal data are transferred to another specific country, to a part of its territory, or to one or more sectors of particular activities in that country, or to an international organisation, the conditions laid down in Articles 63–72 of the Law on Personal Data Protection must be met for such processing to be lawful.

Pursuant to Article 5, paragraph 2 of the Law on Personal Data Protection, the controller bears responsibility for its actions and must be able to demonstrate compliance of the specific processing operation with the Law. The Commissioner, in accordance with the powers conferred by law, adopts a position on specific cases of processing only within proceedings conducted under those same powers (inspection supervision proceedings, proceedings on a complaint, proceedings for issuing special authorisation for the transfer of personal data, etc.), and on the basis of all facts established in the course of such proceedings.

Case Number: 073-14-5599/2024-02

3.5. May a school, acting as a controller, allow a company that owns the software to have access to pupils' data?

Question: A primary school has requested an opinion, stating that a certain software provider has offered the school "the use of software that enables the implementation and record-keeping of enhanced educational and socially useful work, all records related to disciplinary proceedings (a decision to initiate proceedings, a summons for a hearing, minutes from the main hearing, a decision imposing a measure), as well as software that enables the recording of pupils' competition results". It is further stated that the contract provides the service provider with the possibility of accessing the documentation generated by the school using the software, and that the provider undertakes not to disclose or use the data for any purpose. The Commissioner has therefore been asked the following question: "May the school, as the controller of the data, allow the said company to access data that are considered personal and protected by law (pupil's name and surname, personal identification number, address, information about parents)?"

In cases of processing where, for example, a controller–processor relationship exists, the mutual relations between the controller and the processor are regulated in the manner prescribed by Article 45 of the Law on Personal Data Protection. Thus, among other things, Article 45, paragraph 1 of the Law stipulates that where processing is carried out on behalf of the controller, the controller may designate as a processor only such a person or public authority that provides full guarantees regarding the application of appropriate technical, organisational and staffing measures, in a manner that ensures that the processing is performed in accordance with the provisions of the Law and that the rights of the data subjects are protected. Article 45, paragraph 3 of the Law prescribes that

processing by a processor must be governed by a contract or other legally binding act concluded or adopted in written form, including electronic form, which binds the processor to the controller and which regulates the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, as well as the controller's rights and obligations. The mandatory elements of the contract or other legally binding act referred to in paragraph 3 of this Article are prescribed in Article 45, paragraph 4 of the Law.

In this regard, we first note that the purpose of introducing the software by the school is not clear, nor the manner in which the software would be used, nor its technical characteristics, nor whether the school's implementation of such software would be in accordance with the regulations governing education and upbringing. Furthermore, it is not clear what types of personal data would be processed through the software, which categories of individuals would be included, what the roles of all entities involved in the processing would be, nor any other relevant aspects necessary for determining whether the conditions for lawful processing of personal data are met.

The Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018) regulates, in a systemic manner, the general principles and rules of processing that controllers and other entities involved in personal data processing must adhere to, while processing is also regulated by special regulations governing a specific sector or activity.

In this respect, the processing of personal data in the field of education is regulated by special regulations, such as the Law on the Fundamentals of the Education System and other regulations in the area of education and upbringing. Matters relating to enhanced educational and socially useful work, as well as disciplinary procedures, are regulated by these sectoral regulations, which also determine the types of records kept by schools, the manner of collecting data for those records, data retention periods, data recipients, and more. Since the Ministry of Education is responsible for supervising the implementation of regulations in the field of education and upbringing, you may contact that Ministry to obtain an opinion on the application of those regulations in the case described.

From the standpoint of the Law on Personal Data Protection, we generally note that when several different entities participate in a processing operation, it is first necessary to determine the role of each of them (e.g., controller / joint controllers / processor), so that the provisions of the Law may be correctly applied and all corresponding obligations fulfilled.

Article 4, point 3 of the Law on Personal Data Protection prescribes that processing of personal data means any operation or set of operations

performed, whether by automated or non-automated means, on personal data or sets of personal data, such as collection, recording, sorting, grouping or structuring, storage, adaptation or alteration, disclosure, access, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, comparison, restriction, erasure or destruction.

Pursuant to Article 4, points 8 and 9 of the Law on Personal Data Protection, a controller is a natural or legal person, or a public authority, which alone or jointly with others determines the purpose and means of processing; the law determining the purpose and means of processing may also designate the controller or prescribe the conditions for its designation. A processor is a natural or legal person, or a public authority, which processes personal data on behalf of the controller. If two or more controllers jointly determine the purpose and means of processing, they are considered joint controllers (Article 43, paragraph 1 of the Law).

Accordingly, when several different entities participate in a particular processing operation, it is first necessary to correctly determine the role of each of them within the meaning of the Law, taking into account all relevant circumstances of the specific case. These include, in particular, the legal basis, the special regulations governing the processing in that specific context, the purpose of the processing, the manner and nature of the processing, the type of data/processing operations, the duration of the processing, and other relevant factors. We emphasise that, where the relationship between a controller and a processor is concerned, the provisions of Article 45 of the Law must be taken into account, including those relating to the selection of the processor, the form of the contract or other legal act, the content of the contract, and other applicable requirements.

In addition to the above, we note that, under the Law, the controller and the processor are obliged to implement appropriate technical, organisational and staffing measures in order to ensure a level of security appropriate to the risk, taking into account all circumstances in which the processing would be carried out. In this regard, particular attention must be paid to the fact that where sensitive categories of individuals are concerned (for example, minors), the risks arising from the processing are inherently higher. It is therefore necessary to assess the impact of such risks on the rights and freedoms of those individuals.

Appropriate personal data protection measures must be applied at the earliest stage—during the planning, integration and establishment of a given system, that is, at the stage when the means and manner of processing are being determined. At the same time, adequate protection must also be ensured continuously throughout the entire duration of the personal data processing, and the effectiveness of specific protection measures must be

continuously monitored and reassessed for as long as the processing takes place.

We additionally note that, pursuant to Article 57, paragraph 1 of the Law, the controller is obliged to involve the data protection officer in a timely and appropriate manner in all activities relating to personal data protection. Furthermore, the data protection officer appointed by the controller is required, inter alia, to inform and advise the controller, as well as the employees who carry out processing activities, about their statutory obligations in relation to personal data protection, in accordance with Article 58, paragraph 1, point 1 of the Law.

Case Number: 073-14-5629/2024-02

3.6. Is a school obliged to provide the Ministry of Defence with data on male pupils of a certain age group, and is it required to obtain the consent of parents/pupils?

Question: An opinion has been requested on "whether the School is obliged to provide the Ministry of Defence with data on male pupils born in 2007 who attend the grammar school", namely the pupils' name, parent's name, surname, personal identification number, and place and address of residence, as well as an opinion on "whether the School, if it is obliged to provide these data, must obtain the written consent of the parents or the pupils (given that the pupils are over 15 years of age)".

In that regard, and assuming that your question relates to the submission of data to the Ministry of Defence for the purpose of military registration, we inform you as follows.

First, we note that military and conscription obligations, as well as the keeping of military records, are regulated by the provisions of the Law on Military, Labour and Material Obligation ("Official Gazette of the RS", Nos. 88/09, 95/10 and 36/18). The Regulation on the Manner and Procedure for Performing Military, Labour and Material Obligation ("Official Gazette of the RS", Nos. 100/11, 60/15 and 40/19) further regulates the manner and procedure for carrying out these obligations. Article 4 of the Law on Military, Labour and Material Obligation provides that a military obligor is a person who is subject to military obligation under this Law, including, among others, a conscript. Article 5 further prescribes that the Ministry of Defence, through its territorial bodies, ensures and implements military obligations. Articles 14 and 15 of the same Law stipulate that the conscription obligation is carried out, among other things,

through military registration, and that conscripts are entered into the military records at the beginning of the calendar year in which they turn 18. Article 74 of the Law prescribes that, upon the request of territorial bodies, state authorities, authorities of autonomous provinces, local self-government bodies, commercial companies and other legal entities are obliged to provide the data necessary for maintaining the records, as well as to update data concerning changes in the records that fall within their competence.

Furthermore, we note that, pursuant to Article 8 of the Regulation on the Manner and Procedure for Performing Military, Labour and Material Obligation, the Ministry of Defence's Local Self-Government Centre, in accordance with the law, obtains data on conscripts who are subject to military registration from the competent state authorities, local self-government bodies, commercial companies and other legal entities, namely: the name, one parent's name, surname, unique personal identification number, place, municipality and country of birth, and the address and place of residence.

In line with the above and bearing in mind that the Commissioner is not competent for the application of the aforementioned laws and regulations in that field, we direct you to the Ministry of Defence, as the competent authority, for an opinion on their application.

Additionally, we note that the education system and the manner of operation of educational institutions, the records and registers maintained by educational institutions, and other matters relating to the education system are governed by special regulations, namely the Law on the Fundamentals of the Education System, the Law on Secondary Education, and other relevant regulations in this area. Since supervision over the implementation of these regulations lies with the Ministry of Education, you may contact that authority regarding this matter.

The Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18), the implementation of which is overseen by the Commissioner, regulates in a systemic manner the principles of personal data processing and other rules and obligations for controllers and other entities involved in processing, while the processing of personal data in specific fields/activities is regulated by special laws whose implementation is ensured by other authorities.

From the standpoint of the Law on Personal Data Protection, and given that disclosure of personal data, whether by transmission or by otherwise making them available, constitutes a processing operation within the meaning of Article 4, point 3 of the Law, we note that for such processing to be lawful it is necessary, first, to ensure that it is carried out in accordance with the special regulations governing the relevant field/activity, and to

ensure that an appropriate legal basis exists within the meaning of Article 12 of the Law. Furthermore, the processing must be carried out in accordance with the principles of processing set out in Article 5 of the Law, as well as the other applicable rules and obligations prescribed by the Law, depending on the circumstances of each particular case.

In accordance with the above, the Commissioner is of the opinion that, when deciding whether the conditions for disclosing personal data to another entity are met in a given case, the controller must first take into account the provisions of the law and, where applicable, other relevant regulations that establish its powers and obligations, and, depending on the context of the intended processing, the provisions of the law and any other relevant regulations governing the powers and obligations of the entities in the relevant area of social relations.

If the controller determines that a specific law establishes an obligation to disclose certain personal data it processes to another entity, the controller is required, when carrying out such processing, to apply the processing principles set out in Article 5 of the Law on Personal Data Protection, as well as to fulfil the other obligations prescribed by that Law. We note that Article 12 of the Law on Personal Data Protection prescribes the possible legal bases for processing personal data alternatively, meaning that processing is lawful if any one of the prescribed conditions is met; it is not necessary to combine multiple legal bases. Therefore, where the legal basis for processing arises from a specific law, the data subject's consent is not required.

In accordance with the principle of "accountability" set out in Article 5, paragraph 2 of the Law, the controller bears responsibility for the proper application of the Law. It is therefore the controller who must decide whether, in a particular case, the conditions for lawful processing of personal data are met, and the controller is required, when conducting the processing, to comply with all processing principles and other obligations prescribed by the Law.

We also note that, pursuant to Article 57, paragraph 1 of the Law, the controller is obliged to involve the data protection officer in a timely and appropriate manner in all activities relating to personal data protection. Furthermore, the data protection officer appointed by the controller has, among other duties, the obligation to inform and advise the controller or processor, as well as the employees who carry out processing activities, of their legal obligations in relation to personal data protection, in accordance with Article 58, paragraph 1, point 1 of the Law.

Case Number: 073-14-5611/2024-02

3.7. Possibility for a social welfare centre to install a camera in a room used for "supervised contact sessions"

Question: The Centre for Social Work contacted the Commissioner regarding its intention to install a camera, as stated, in a "room for supervised contact sessions", in order "to maintain control and ensure the safety of the contact by the professional worker at all times". It is further stated that the camera "does not store or retain recordings; it only transmits a live image and sound, and only when connected via an application on a tablet. The tablet connected to the camera would be accessible solely to the professional worker responsible for supervising the contact, and only during the contact session, in case it is necessary for the worker to leave the room in which the session is taking place." An opinion has been requested from the Commissioner as to whether "such use of a camera" is in accordance with the Law on Personal Data Protection.

From the standpoint of personal data protection, we generally point out that the use of video and/or audio surveillance may significantly endanger the privacy and other rights and freedoms of individuals, particularly when sensitive categories of persons are involved, such as children and minors, as well as potentially sensitive types of personal data, bearing in mind the nature of the activity in connection with which the introduction of the video/audio surveillance is envisaged. Accordingly, the controller is obliged, when deciding whether to introduce such surveillance, to determine whether the video/audio monitoring is genuinely necessary or whether the purpose for which it is being introduced could be achieved by some other means that is less intrusive to privacy and other fundamental rights and freedoms of the individuals concerned. Furthermore, before commencing any processing of personal data, the controller must establish that all necessary conditions for the lawfulness of such processing have been met.

First, we note that the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18) does not contain specific provisions on video or audio surveillance.

Namely, the Law on Personal Data Protection regulates, in a systemic manner, the principles and general rules of processing and the corresponding obligations that controllers and other entities involved in the processing of personal data must comply with, while processing in a specific sector/activity is regulated by special regulations, the application of which is overseen by other authorities.

In view of the above, we point out that procedures relating to family matters are regulated by special laws, such as the Family Law and others,

while matters concerning the establishment and operation of social welfare institutions, supervision of the work of social welfare institutions, inspection supervision in the performance of social welfare activities, support and improvement of the quality of professional work in the social welfare system, and other issues of importance for social welfare, are regulated by the Law on Social Welfare and other relevant regulations. Since matters of public administration relating to the system of family-law protection fall within the competence of the Ministry for Family Welfare and Demography, while the implementation of the Law on Social Welfare falls within the competence of the Ministry of Labour, Employment, Veteran and Social Affairs, you may contact these authorities to obtain an opinion on the application of those regulations in the described case.

However, as the use of a video/audio surveillance system involving individuals constitutes the processing of those individuals' personal data within the meaning of Article 4(3) of the Law on Personal Data Protection, we generally highlight several key aspects of personal data processing that must be taken into account.

Namely, all processing of personal data is subject to the processing principles prescribed in Article 5 of the Law, specifically the principles of: "lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation", and "integrity and confidentiality" (Article 5, paragraph 1 of the Law).

Furthermore, an appropriate legal basis must be ensured for every processing of personal data, in accordance with Article 12, paragraph 1, points 1–6 of the Law.

Therefore, for the processing of personal data to be lawful, it is first necessary to ensure that it is carried out in accordance with the special regulations governing the relevant field/activity; that the purpose of the processing is specifically defined, explicit, justified and lawful; that an appropriate legal basis exists within the meaning of Article 12 of the Law; and that the processing is carried out in accordance with the processing principles from Article 5 of the Law and other applicable rules and obligations prescribed by the same Law, depending on the circumstances of each individual case.

We note that if the processing is carried out for the purpose of complying with the controller's legal obligations (Article 12, paragraph 1, point 3 of the Law) or for the performance of tasks carried out in the public interest or the exercise of powers vested in the controller by law (Article 12, paragraph 1, point 5 of the Law), the basis for such processing is determined by law. Accordingly, the legal basis for processing carried out by public authorities in the performance of their duties and powers must derive from the relevant special laws and other regulations.

We note that if the controller decides to commence the processing of personal data, it thereby assumes various obligations that must be fulfilled in order to document the compliance of that processing with the Law on Personal Data Protection. These include, among others: taking appropriate personal data protection measures when determining the means of processing as well as during the processing itself (Articles 41 and 42 of the Law); keeping records of processing activities (Article 47 of the Law); conducting a data protection impact assessment of the envisaged processing operations (Article 54 of the Law); seeking the Commissioner's prior opinion where the impact assessment indicates that the intended processing is likely to result in a high risk unless measures are undertaken to mitigate that risk (Article 55 of the Law) etc:

The cases in which the controller is obliged to carry out a data protection impact assessment are prescribed in Article 54, paragraph 4 of the Law, as well as in the Decision on the List of Types of Personal Data Processing Operations for which a Data Protection Impact Assessment Must Be Conducted and an Opinion Requested from the Commissioner for Information of Public Importance and Personal Data Protection ("Official Gazette of the RS", Nos. 45/19 and 112/20).

Therefore, in line with the principle of accountability under Article 5, paragraph 2 of the Law on Personal Data Protection, the controller bears responsibility for the proper application of the Law. The decision to initiate any processing of personal data is made independently by the controller, taking into account all of the above, and, if the controller decides to begin a particular processing operation, it must be able to demonstrate compliance of that processing with the Law.

Furthermore, we note that, pursuant to Article 57, paragraph 1 of the Law, the controller is obliged to involve the data protection officer in a timely and appropriate manner in all activities relating to personal data protection. In addition, the data protection officer appointed by the controller has, inter alia, the duty to inform and advise the controller or processor, as well as the employees who carry out processing activities, of their legal obligations concerning personal data protection, in accordance with Article 58, paragraph 1, point 1 of the Law.

We emphasise that this opinion is of a general nature, given that the Commissioner cannot take a position on individual cases of personal data processing outside the proceedings conducted in accordance with the Commissioner's statutory powers (proceedings on a complaint, inspection supervision proceedings, etc.), as doing so would prejudge the Commissioner's decision in such proceedings. This opinion likewise does not extend to matters governed by other regulations whose implementation does not fall within the competence of this authority.

Case Number: 073-14-5730/2024-02

3.8. Deletion of data from a medical record

Question: An individual has requested an opinion, stating, among other things: "after being dissatisfied with the work of a certain private medical institution, I decided to close my medical file with them", and that he requested a copy of the history of his "treatment and examinations there". The individual also requested that his treatment history and data about him be deleted from their system and received the following reply: "Unfortunately, it is not possible to delete your history from the system because these are medico-legal documents and we must keep them in case a dispute arises and the court issues an order for them." In this regard, the individual has asked the Commissioner "whether this assertion is correct, and if so, I am specifically interested in which data the medical institution may retain about me, for how long, and on what legal basis and under which article of the law."

In this respect, it should be borne in mind that the processing of personal data in the field of healthcare — including matters relating to access to medical documentation, its collection and disclosure, patients' rights to data confidentiality, and other related issues — is regulated by special laws in this area, such as the Law on Healthcare, the Law on Patients' Rights, and the Law on Health Documentation and Records in the Field of Healthcare. Among other things, this latter law sets out the retention periods within which healthcare institutions, including private practices, must keep medical documentation and the prescribed records.

Accordingly, when a healthcare institution, as a controller, processes personal data in accordance with special laws that establish a legal obligation to process certain personal data — which includes retaining such data for the periods prescribed by law — the controller is not required to delete the personal data in such cases.

In this regard, we first note that the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018), the implementation of which falls within the competence of the Commissioner, regulates in a systemic manner the principles of personal data processing, as well as other general rules and certain obligations for controllers and other entities involved in processing. Processing of personal data in the relevant fields/activities is regulated by special laws, the implementation of which is overseen by other authorities.

Supervision over the implementation of the aforementioned regulations in the field of healthcare does not fall within the competence of the Commissioner but rather within the competence of the Ministry of Health. You may therefore contact that Ministry in order to obtain an opinion on the application of those regulations in the described case.

From the standpoint of the Commissioner's competence in the field of personal data protection, we generally point out the following.

The Law on Personal Data Protection regulates certain rights of individuals whose data are processed, such as: the right of access to data, the right to rectification and supplementation, the right to erasure of personal data, and others. These rights are exercised in the manner and according to the procedure prescribed by the said Law. This specifically means that, if an individual wishes to exercise any of the aforementioned rights under that Law, he or she must contact the controller directly, i.e. the entity that processes (which includes retaining) his or her personal data in the given case. Upon receiving such a request, the controller, taking into account the circumstances of the specific case and in particular the provisions of the special regulations governing a given type of personal data processing, must decide on the submitted request. If the controller fails to act upon the submitted request, or if, after receiving the requested information, the individual considers that the processing of his or her personal data is being carried out contrary to the provisions of the Law on Personal Data Protection, he or she has the right, in accordance with Article 82 of that Law, to lodge a complaint with the Commissioner. The individual may also seek appropriate judicial protection by filing a claim with the competent High Court, in accordance with Article 84 of the Law.

In addition to the above, it should be borne in mind that the rights of individuals established by the Law on Personal Data Protection are not absolute rights, and may, exceptionally, be restricted in the cases prescribed by Article 40 of the Law.

We further note that the right of access to data (Article 26 of the Law) means that the data subject has the right to request from the controller information as to whether his or her personal data are being processed, access to those data, as well as information on the purpose of processing, the types of data being processed, the recipients, the data retention period, the existence of the right to request from the controller the rectification or erasure of personal data, and other relevant information.

With regard to the right to erasure of personal data, this right is regulated by Article 30, paragraph 1 of the Law, according to which the data subject has the right to have his or her personal data erased by the controller. Paragraph 2 of the same Article sets out the cases in which the controller is obliged to erase such data (for example, the data are no longer necessary for achieving the processing purpose, the data subject has withdrawn consent, etc.).

However, as already emphasised, these rights — including the right to erasure — are not absolute, and the controller is not always obliged to erase personal data, particularly in cases provided for in Article 30, paragraph 5 of the Law. Such cases include, for example, situations in which

processing is necessary, and to the extent necessary, for compliance with a legal obligation of the controller requiring processing, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; for the fulfilment of public interest in the field of public health, in accordance with Article 17, paragraph 2, points 8) and 9), as well as in other prescribed situations.

We note that this opinion is of a general nature, bearing in mind that the Commissioner, in accordance with his statutory competences, may take a position on specific cases of personal data processing only within the framework of proceedings conducted pursuant to his statutory powers (complaint proceedings, inspection supervision, etc.), and only on the basis of all the facts and circumstances established in such proceedings.

Furthermore, this opinion does not extend to matters regulated by other legislation whose implementation does not fall within the competence of the Commissioner, including the manner and procedure for exercising certain rights in accordance with other regulations (for example, the Law on Patients' Rights, etc.).

Case Number: 073-14-19/2025-02

3.9. Speech-therapy application – processing of special categories of personal data; obligations of controllers and other participants in the processing

The question: An opinion has been requested in relation to an application being developed by the applicant, intended for speech therapists and parents, noting that it involves the processing of users' personal data, including data relating to children. In this regard, the following questions have been raised: "Is it necessary to obtain explicit consent from parents or guardians for the processing of data relating to children under the age of 15, and what is the best way to document such consent? What security measures are recommended for storing and processing sensitive data, particularly in the context of an application that stores data about children and their speech-therapy treatments, and possibly additional information on existing illnesses/difficulties? How should one proceed in the event of a data breach, and within what timeframe must the Commissioner and users be notified? If services of providers located outside Serbia are used… what obligations apply with respect to international data transfers…?"

Taking into account your questions, from the standpoint of personal data protection we hereby outline, in general terms, some of the most important aspects of personal data processing that must be observed.

Namely, in accordance with the Law on Personal Data Protection, certain conditions must be met for the processing of personal data to be permissible. This means that controllers must first take into account the special regulations applicable in the relevant field (e.g. healthcare, education, social protection…), that is, they must primarily determine whether the processing they intend to carry out would be in compliance with those regulations — in the case you describe, the regulations governing the provision of speech-therapy services — taking into consideration both the legal obligations of the service provider and the rights of the service users.

Furthermore, the purpose of the processing of personal data must be specifically defined, explicit, justified, and lawful, and the processing must be necessary — that is, genuinely required — for achieving that purpose. An appropriate legal basis for the processing must then exist in accordance with Article 12 of the Law, and the scope and type of data processed must be adequate and proportionate to the purpose, in line with the principle of data minimisation, while also respecting the other processing principles under Article 5 of the Law, including transparency of processing. It must also be borne in mind that the processing of special categories of personal data (e.g. data concerning health) is subject to a restrictive processing regime; such data may be processed only where one of the statutory exceptions permitting the processing of these data is fulfilled.

Consent to processing is one of the six possible legal bases for the processing of personal data. Article 4, paragraph 1, point 12) of the Law defines this term and stipulates that the consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which that person, by a statement or by a clear affirmative action, gives consent to the processing of personal data relating to him or her. Consent therefore requires an active action by the individual, through which the person unmistakably expresses his or her will — i.e. consent to the processing of his or her personal data — after having been informed by the controller of all relevant aspects of the intended processing, in accordance with the principle of transparency laid down in Article 5 of the Law.

Furthermore, Article 15 of the Law prescribes specific conditions that must be met for processing based on consent to be considered lawful. Among other things: the controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data; if consent is given in the context of a written statement that also concerns other matters, the request for consent must be presented in a manner that clearly distinguishes it from those other matters, in an intelligible and easily accessible form, using clear and plain language; before giving consent,

the data subject must be informed of the right to withdraw consent and of the consequences of such withdrawal, and the withdrawal must be as easy as giving consent; etc. When assessing whether consent has been freely given, particular consideration must be given to whether the performance of a contract, including the provision of services, is being made conditional on consent that is not necessary for its performance (Article 15, paragraph 4 of the Law).

As already noted, the processing of special categories of personal data, which includes data concerning health, is subject to a restrictive regime. Such processing is, as a rule, prohibited (Article 17, paragraph 1), and is permitted only exceptionally, in the cases exhaustively listed in Article 17, paragraph 2, points 1) to 10). These include, inter alia, situations in which the data subject has given explicit consent for the processing for one or more specified purposes, unless a law prescribes that the processing shall not be carried out on the basis of consent.

In accordance with the above, if the controller intends to base the processing of special categories of personal data on the data subject's consent, such consent must be explicit, which, among other things, entails an appropriate manner in which the individual expresses his or her will — i.e. consent to the processing. One possible way of ensuring explicit consent would be the explicit confirmation of consent through a written statement. However, this need not always be the only possible method of obtaining explicit consent; rather, depending on the circumstances and facts of each individual case, it must be assessed whether the consent would be valid — that is, a lawful and effective legal basis for processing. The individual must also be informed, in an appropriate manner, of all relevant aspects of the personal data processing, presented in a clear and easily accessible way, using plain and simple language, particularly where the information is intended for a minor.

In accordance with the principle of "accountability" under Article 5, paragraph 2 of the Law, the burden of proof always lies with the controller, who must be able to demonstrate that the processing it carries out is compliant with the Law, including proving that it is based on valid consent.

Article 16 of the Law stipulates that a child under the age of 15 may not independently give consent to the controller for the processing of personal data relating to him or her in the context of the use of an information society service; such consent must instead be given by the parent exercising parental responsibility or by another legal representative of the child. The controller must take reasonable measures to verify whether consent has indeed been given by the parent exercising parental responsibility or by another legal representative of the minor, taking into account available technologies.

Furthermore, we note that, in accordance with the obligation under Article 41 of the Law, the controller must implement appropriate technical, organisational and staffing measures in order to ensure that the processing is carried out in compliance with the Law and must be able to demonstrate such compliance, taking into account the nature, scope, context and purposes of the processing, as well as the likelihood and severity of the risks to the rights and freedoms of natural persons. These data protection measures must be reviewed and updated where necessary, and where proportionate to the processing they may include the adoption and application of appropriate internal acts on data protection by the controller.

The controller is obliged, both when determining the means of processing and throughout the processing itself, to apply appropriate technical, organisational and staffing measures (e.g. pseudonymisation) aimed at ensuring the effective application of data protection principles (e.g. data minimisation). The controller must also ensure the implementation of the necessary safeguards during the processing in order to meet the requirements of the Law and to protect the rights and freedoms of the data subjects.

Appropriate personal data protection measures must be applied at the earliest stage — during the planning, integration and establishment of a system, that is, at the stage when the means and manner of processing are first being determined. However, adequate protection must also be ensured continuously, throughout the entire duration of the personal data processing, and the effectiveness of particular safeguards must be monitored and reassessed throughout the entire life cycle of the system.

The Law prescribes what personal data protection measures may include, and such measures may, in particular, consist of: 1) pseudonymisation and encryption of personal data; 2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 3) the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident; 4) a process for regularly testing, assessing and evaluating the effectiveness of technical, organisational and staffing measures for ensuring the security of processing.

When assessing the appropriate level of security for personal data, controllers are obliged to take into particular consideration the risks associated with the processing, especially the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that have been transmitted, stored or otherwise processed (Article 50, paragraph 3). Where personal data relating to sensitive categories of individuals (e.g. children, minors, patients) and/or special

categories of personal data (e.g. data concerning health) are processed, such processing inherently carries a higher risk to the rights and freedoms of the individuals concerned. Consequently, it will require additional caution when determining appropriate data-protection measures, in order to achieve an adequate level of security for the processing.

Notification of the Commissioner and of the data subjects regarding a personal data breach is regulated by Articles 52 and 53 of the Law, which prescribe the deadlines within which such notification must be submitted (72 hours from becoming aware of the breach, etc.), as well as other corresponding obligations in this respect.

We also note that, where several entities participate in a particular processing operation, it is necessary to determine their roles in relation to that processing (e.g. controller, joint controllers, processor), and that their mutual relationships must be appropriately regulated depending on those roles (e.g. a data processing agreement). In this regard, if personal data are transferred to other countries or international organisations, the conditions relating to data transfers set out in Articles 63–72 of the Law must also be fulfilled. At the same time, it must be borne in mind that, for any data transfer, all other requirements must also be met — the existence of an appropriate legal basis and a lawful processing purpose, transparency, data minimisation and the other processing principles, as well as all other obligations established by the Law. All of these elements must be assessed in light of the facts and circumstances of the specific case.

We also draw attention to the obligation of controllers who intend to initiate processing that is likely to result — particularly where new technologies are used and taking into account the nature, scope, context and purpose of the processing — in a high risk to the rights and freedoms of natural persons, to carry out, before commencing the intended processing, a data protection impact assessment of the envisaged processing operations. The cases in which such an assessment is mandatory are set out in Article 54 of the Law and in the Decision on the List of Types of Personal Data Processing Operations for which a Data Protection Impact Assessment Must Be Performed and an Opinion Requested from the Commissioner ("Official Gazette of the RS", Nos. 45/2019 and 112/20).

Case Number: 073-14-243/2025-02

3.10. "Privacy Policy" and deletion of data

Question: An opinion has been requested regarding a privacy policy which, as the applicant states, "will represent a condition for using the services that I will provide through the website (IT services)", and further notes that "users will be required to accept the terms set out in the Privacy Policy in order to be able to use the services… my question relates to Article 30 of the Law on Personal Data Protection… is it sufficient to provide general criteria for determining retention periods (e.g. personal data are retained solely for the purpose of initiating, exercising or defending a legal claim, for a period of 10 years from the date of the last processing operation, which represents the general statutory limitation period), having in mind Article 23, paragraph 2, point 1 of the Law?" The applicant further asks: "In the event that a user requests the deletion of his or her data and information on the legal basis and retention period following such a request, am I obliged to provide exact retention periods, or is it sufficient to refer to the provision in the Privacy Policy that defines general criteria… is it sufficient to inform the user that their data will be retained solely for the purpose of a potential legal proceeding, and for the periods prescribed by law, e.g. 5 years in the event of damages, 10 years for claims, etc.?"

In this regard, we note that, where personal data are collected from the data subject, the controller is obliged, at the moment of collecting the personal data, in accordance with Article 23, paragraph 1 of the Law on Personal Data Protection, to provide that person with the prescribed set of information, as well as the additional information required under Article 23, paragraph 2 of the Law (e.g. the data retention period, or, if this is not possible, the criteria used to determine it; the existence of the right to request access to, rectification or erasure of personal data, etc.), which may be necessary in the specific case to ensure fair and transparent processing in relation to the data subject.

It should first be noted that the Law on Personal Data Protection regulates, in a systematic manner, the principles of personal data processing, as well as other general rules and obligations, while the processing of personal data within relevant areas of social life/activities is regulated by special laws, the application of which is overseen by other competent authorities.

From the perspective of personal data protection, we emphasise that, for a particular processing operation to be permitted, the purpose of the processing must be specifically defined, explicit, justified and lawful; the processing must be carried out in accordance with special regulations governing the relevant area/activity; there must be an appropriate lawful basis

for processing within the meaning of Article 12 of the Law; and the processing must be carried out in accordance with the principles laid down in Article 5 of the Law and other applicable rules and obligations prescribed by the Law, all depending on the facts and circumstances of each individual case.

We note that it is the responsibility of controllers to determine the appropriate method for ensuring the exercise of the right to be informed, i.e. to decide independently on the specific manner in which they will provide the data subject with all information required by the Law, including situations where this is done through privacy policies published, for example, on a website, while taking into account all relevant aspects of the processing, as well as ensuring that the information is easily accessible and understandable to individuals (using clear and simple language, etc.).

In relation to the question concerning personal data retention periods, we note that, where such periods are not determined by the relevant special regulations, they are defined by the controller, taking into account the nature, scope and purpose of the processing or the type of processing, and applying the general processing principles laid down in Article 5 of the Law. These principles stipulate, inter alia, that personal data must be stored in a form which permits the identification of data subjects only for as long as is necessary to achieve the purpose of the processing (storage limitation), and that personal data must be collected for purposes that are specifically defined, explicit, justified and lawful and must not be further processed in a manner incompatible with those purposes (purpose limitation).

Accordingly, personal data shall be retained only for the period that is genuinely necessary to achieve the purpose of the processing, in accordance with Article 5(1)(5) of the Law. Once the purpose has been fulfilled, the need to retain the relevant data ceases. We note that, where retention periods are prescribed by special regulations governing processing in a particular sector or field, the controller is, in such cases, obliged to comply with the statutory retention periods.

With regard to the right to erasure of personal data, this right is regulated by Article 30(1) of the Law, pursuant to which the data subject has the right to have his or her personal data erased by the controller. Furthermore, paragraph 2 of the same Article prescribes the circumstances in which the controller is obliged to erase such data (e.g. the data are no longer necessary for the achievement of the purpose of the processing, the data subject has withdrawn consent, etc.).

However, it should also be borne in mind that the rights of individuals established by the Law on Personal Data Protection are not absolute rights, including the right to the erasure of personal data. Namely, the controller is not obliged to erase personal data if one of the situations prescribed by Article 30(5) of the Law applies, such as, for example, where the processing is necessary, and to the extent that it is necessary, for compliance with the controller's legal obligation requiring the processing, as well as in other prescribed cases.

Given that accountability lies with the controller, it is the controller who must be able to demonstrate, i.e. present evidence of, the compliance of the intended processing with the Law (Article 5(2) of the Law). The burden of proof that personal data are processed in accordance with the Law — and therefore in accordance with the principles of lawfulness, fairness and transparency, the principle of purpose limitation, and the principle of storage limitation — always lies with the controller. This must also be taken into account when deciding how exactly these principles will be implemented in practice.

We further note that every controller applies the provisions of the Law on Personal Data Protection autonomously, just as it applies the provisions of any other regulation, taking into account all relevant circumstances under which a specific personal data processing operation is carried out within its organisation.

Case Number: 073-14-665/2025-02

3.11. Video surveillance in vehicles – use of technologies such as GPS, biometrics, artificial intelligence

Question: The commercial company "intends, for the purpose of improving the quality of the service and increasing the safety of users and service providers, to introduce a video-surveillance system in the vehicles used by the service providers, which entails installing cameras with multiple possibilities for recording users and service providers, as well as the external traffic taking place, all of this using artificial-intelligence functionalities… The cameras would automatically detect various events, namely: identification of the service provider by reading his biometric data (facial biometrics), or by inserting an NFC card into the camera, as well as detection of improper behaviour by the service provider (using a mobile telephone, failing to fasten the seatbelt, inattention, drowsiness)… and GPS data on the location of the vehicle, the duration of the service and the number of detected events, and the cameras would also have the capability of audio recording… The recordings from the cameras would be stored on an

SD memory card… all key detected events would be logged and stored on Amazon Cloud and would be located in the territory of Europe for a certain period of time…". In this regard, certain questions have been raised, stating, inter alia, "…given that the intended processing of personal data through camera recording represents the use of new technologies, we consider that, pursuant to Article 54 of the Law on Personal Data Protection and the Decision on the List of Activities…, it is mandatory to carry out a data-protection impact assessment… we kindly ask you to send us a sample template showing what the impact assessment should look like…", and this authority has been requested to provide an opinion so that "we can be certain that the entire plan for introducing the video-surveillance system by the Controller will be in compliance with the applicable legislation and best practice in this field", as well as to indicate to the applicant anything else that this authority considers significant, from the standpoint of personal-data protection, "in relation to the situation at hand".

In this regard, we point out that the Law on Personal Data Protection prescribes a category of special types of personal data, which include, inter alia, biometric data, the processing of which is, as a rule, prohibited under Article 17(1) of the Law, and is exceptionally permitted only in the cases exhaustively set out in paragraph 2 of the same Article of the Law. In this sense, it should be borne in mind that employees have the right to privacy in the workplace, so the employer, as the Controller, may not pursue the defined purpose of data processing in a manner that excessively interferes with employees' privacy, particularly if that purpose can be achieved in another, less intrusive manner for employees' privacy. Therefore, in cases where the personal data are not adequate and proportionate and not limited solely to what is necessary in relation to the defined purpose of processing, such processing cannot be considered permissible from the standpoint of the Law on Personal Data Protection.

In this connection, we inform you of the following.

First, we point out that the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018) does not contain specific provisions on video and audio surveillance, nor provisions on the use of artificial intelligence.

The Law on Personal Data Protection, the implementation of which falls within the competence of the Commissioner, regulates in a systemic manner the principles of personal data processing, as well as other general rules and specific obligations for Controllers and other entities, while the processing of personal data in the relevant fields/activities is regulated by special regulations, the application of which is supervised by other authorities.

In this regard, we note that the performance of activities related to the protection of persons, property and business operations through physical

and technical protection is regulated by the provisions of the Law on Private Security. Pursuant to Article 30(1) of this Law, "video protection" is prescribed as one of the possible means of technical protection, and the provisions of this Law also prescribe the manner in which such protection may be carried out. Bearing in mind that Article 70 of the Law on Private Security stipulates that oversight of the application of this Law is exercised by the Ministry of the Interior, we note that, for the purpose of obtaining an opinion on the application of the provisions of that Law, you may contact this Ministry, as the competent authority in that field.

Additionally, and having regard to the statements made in your email, we point out that issues relating to traffic safety and the transport of passengers are regulated by the provisions of the Law on Road Traffic Safety and the Law on Passenger Transport in Road Traffic, the application of which is supervised by the Ministry of the Interior and the Ministry of Construction, Transport and Infrastructure respectively.

We further note that, pursuant to Article 91 of the Law on Personal Data Protection, the processing of personal data in the field of labour and employment is governed by the provisions of the laws regulating labour and employment and by collective agreements, alongside the application of the provisions of this Law, and that the rights, obligations and responsibilities arising from an employment relationship, or on the basis of work, are regulated by the provisions of the Labour Law and other relevant regulations in the field of labour and employment, the implementation of which does not fall under the competence of the Commissioner. Consequently, we note that, regarding the application of these regulations, you may contact the Ministry of Labour, Employment, Veteran and Social Affairs.

However, since the recording of natural persons through video and audio surveillance constitutes an act of personal data processing within the meaning of Article 4(3) of the Law, we generally point out, from the standpoint of this Law, that the processing of personal data through video and audio surveillance must first be in compliance with the special regulations governing the relevant field/activity. It is then necessary to ensure an appropriate legal basis within the meaning of Article 12 of the Law, whereby, in the case of processing special categories of personal data under Article 17(1) of the Law, it is additionally required that the processing fall under one of the cases set out in paragraph 2 of the same Article. Furthermore, the processing must be carried out in accordance with the principles of processing laid down in Article 5 of this Law, as well as other applicable rules and obligations prescribed by this Law, all of which depends on the facts and circumstances of each individual case.

Furthermore, since, in your email, you also raise the question of whether the intended processing would be permissible on the basis of "the con-

sent of service providers and service users", we note that consent is only one of six possible lawful legal bases for the processing of personal data prescribed by Article 12 of the Law. Article 4(1), point 12 of the Law also prescribes and defines this term, whereby "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which that person, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. When assessing whether consent for the processing of personal data has been freely given, particular attention must be paid to whether the performance of a contract, including the provision of a service, is conditional upon the giving of consent that is not necessary for its performance (Article 15(4) of the Law).

Free will is an essential precondition for the validity of consent as a lawful legal basis for the processing of personal data. A declaration of intent by a natural person which cannot be altered or withdrawn without producing legal consequences for that person's position cannot be regarded as valid consent within the meaning of the Law. This is especially relevant in the present case, as the processing involves biometric data, the processing of which is, as noted above, generally prohibited under the Law and allowed only exceptionally, inter alia in the case set out in Article 17(2)(1) of the Law, which stipulates that the processing referred to in paragraph 1 is exceptionally permitted if the data subject has given explicit consent for the processing for one or more specified purposes, unless the Law prescribes that the processing may not be based on consent.

In view of the foregoing, where the processing of employees' personal data is concerned, the employer's authority, as Controller, to carry out the intended processing should primarily derive from the relevant special regulations in the field of labour, employment, etc., alongside the application of the processing principles laid down in Article 5 of the Law, as well as other applicable rules and obligations established by the Law.

Furthermore, given that the use of a video and audio surveillance system may significantly jeopardise the privacy and other rights and freedoms of the persons whose personal data are processed in this manner, we note that Controllers, when deciding whether to introduce video and audio surveillance into a particular area, must, prior to its introduction, ensure that the coverage of the area by the surveillance system (the camera angle) is proportionate to the purpose of processing in the specific case. In other words, the camera should capture only what is necessary to achieve the purpose, while the retention period for personal data must be limited solely to the period necessary to achieve the purpose of processing in the specific case, etc., and in particular whether that purpose could be achieved in another, less intrusive manner for the privacy of the individuals concerned.

We further note that, based on your statements, it is not clear who the "users" are and who the "service providers" are, nor the status of each of the entities that would participate in the intended processing. Namely, when several different entities take part in a particular processing operation, it is first necessary to correctly determine the status of each of them within the meaning of the Law, taking into account all relevant circumstances of the specific case, and particularly the legal basis, the special regulations governing processing in the given situation, the purpose of processing, the manner and nature of processing, the type of data/actions, the duration of processing, etc. Pursuant to Article 4, points 8 and 9 of the Law, a "Controller" is a natural or legal person, or a public authority, which alone or jointly with others determines the purpose and manner of processing, whereas a "Processor" is a natural or legal person, or a public authority, which processes personal data on behalf of the Controller. Article 43(1) of the Law also defines the concept of "joint controllers", stipulating that these are two or more controllers which jointly determine the purpose and means of processing.

With regard to the statements in your email concerning the obligations of the Controller prescribed by Article 54 of the Law, i.e. the "obligation to conduct a data-protection impact assessment", as well as the request to provide "a sample template of what the impact assessment should look like", we indicate that detailed information on all matters related to data-protection impact assessments can be found on the website of the Commissioner, www.poverenik.rs, under the "Data Protection" section, where you can access the "Guidelines for Conducting a Data-Protection Impact Assessment" in the drop-down menu.

Furthermore, regarding the statements in your email indicating that "all key detected events would be logged and stored on Amazon Cloud and would be located in the territory of Europe for a certain period of time", we note that, if personal data are transferred to other countries or international organisations, the conditions prescribed by Articles 63–72 of the Law must be met. In addition, for any transfer of personal data, it must also be ensured that all other conditions laid down by the Law are fulfilled, such as the existence of an appropriate legal basis, explicit and lawful processing purposes, transparency, data minimisation, and other processing principles under Article 5 of the Law, as well as compliance with other applicable obligations prescribed by the Law, depending on the facts and circumstances of each specific case.

Finally, we emphasise that, pursuant to Article 5(2) of the Law, accountability lies with the Controller, i.e. the Controller must be able to demonstrate that the specific processing is compliant with the Law, while the Commissioner, in accordance with the competences established by the Law, may take a position on specific processing cases only within the procedures

conducted in line with its statutory powers (inspection supervision procedures, complaint procedures, etc.).

Case Number: 073-14-37/2025-02

3.12. Possibility of installing a camera for "video recording" of traffic in a vehicle

Question: An opinion has been requested regarding whether the commercial company is processing personal data contrary to the processing principles set out in Article 5(1) of the Law on Personal Data Protection, i.e. point 3 of the Decision on the List of Types of Personal Data Processing for which a Data-Protection Impact Assessment must be carried out and an opinion sought from the Commissioner, in the event that the Company "installs a camera exclusively for video recording of traffic (without audio recording) in the cabin of a passenger vehicle which it owns or during its use, in such a way that the camera is positioned so that it does not record the interior of the passenger-vehicle cabin, and is technically adjusted (focus) so that the shape, colour and size of a vehicle, object or person can be recognised, while symbols on registration plates cannot be identified, nor can a person recorded in public areas be recognised, i.e. the identity of any person who may be recorded is not identifiable". It is further stated that the Company "...conducts continuous monitoring of the vehicles in its fleet... monitors the driving styles of employees who operate the vehicles, implements road-traffic safety and property-protection activities... monitors key indicators of road-traffic safety, including the monitoring of the number of traffic accidents and the parties involved... conducts in-depth analysis in the form of an investigation of each individual traffic accident, etc.", as well as that access to the video recordings obtained from the cameras is granted "only if a traffic accident occurs, or in the event of damage to the Company's vehicle".

It should be borne in mind that the notion of personal data encompasses not only data on the basis of which a person's identity is directly, i.e. immediately, determined, but also cases in which a person's identity can be determined indirectly, that is, in combination with other information, which must be assessed depending on the circumstances and all the facts of the specific case. Particular attention must be paid to this when introducing various technological solutions, including video/audio surveillance.

In this regard, we first note that, based on your submission, it is not possible to determine the exact purpose of introducing the proposed video-

surveillance system, nor the manner in which it would operate, nor what is meant by the term "video recording of traffic", particularly in terms of the area that would be covered and the categories of persons concerned. It is likewise unclear what you mean by monitoring "the driving styles of employees", what the specific purpose of such processing is, and how it would be achieved, nor are other essential aspects of personal-data processing specified, such as the types of personal data, the legal basis for processing, etc.

Bearing in mind your question, we first point out that the very possibility of using video surveillance is not regulated by the legislation falling within the competence of the Commissioner.

On the other hand, the Law on Private Security ("Official Gazette of the RS", Nos. 104/2013, 42/2015 and 87/2018), which, inter alia, regulates the performance of activities relating to the protection of persons and property in cases where such activities do not fall within the exclusive competence of state authorities, prescribes in Article 30(1), as one of the possible means of technical protection, "video protection", and the provisions of this Law further regulate the manner in which such protection may be carried out. Therefore, when video surveillance is introduced for the purpose of protecting persons and property in cases where such activities do not fall within the exclusive competence of state authorities, such video surveillance may be carried out only in the manner and under the conditions set out in the Law on Private Security.

Furthermore, issues relating to road-traffic safety, the competences and responsibilities of traffic-safety entities, the authorisation to record traffic, etc., are regulated by the Law on Road Traffic Safety. Pursuant to Article 286(1) of that Law, the authority competent for police affairs and the authority competent for traffic affairs are authorised to record traffic for the purpose of documenting traffic offences, the behaviour of road users, and for monitoring traffic safety and flow, all within the scope of their competences.

Since the implementation of the Law on Private Security and the Law on Road Traffic Safety falls within the competence of the Ministry of the Interior, you may contact that authority to obtain an opinion on the application of the aforementioned laws in the situation described.

From the standpoint of the Commissioner's competences regarding the application of the Law on Personal Data Protection, we point out that the recording of natural persons through video/audio surveillance unquestionably constitutes personal-data processing, and certain conditions must be met for such processing to be permissible.

Specifically, the purpose of the processing must be clearly defined, explicit, justified and lawful, and the processing must be necessary, i.e. genuinely required to achieve that purpose. There must also be an appropriate legal basis for the processing within the meaning of Article 12 of the Law, and the scope and type of data processed must be adequate and propor-

tionate to the purpose, in accordance with the principle of data minimisation, along with compliance with the other principles laid down in Article 5 of the Law. Controllers must also take into account the special regulations applicable in the specific field and must first determine whether the intended processing would be permissible from the standpoint of those regulations. If the above conditions are not met, the processing cannot be considered lawful under the Law on Personal Data Protection.

From the standpoint of personal-data protection, and speaking generally, we note that the use of video/audio-surveillance systems may significantly jeopardise the privacy and other rights and freedoms of the individuals whose personal data are processed in this manner (e.g. freedom of movement, etc.). Therefore, when deciding whether to introduce video surveillance, Controllers must first take into account the special regulations applicable in the specific case (i.e. whether the introduction of video surveillance is in compliance with those regulations), and then determine whether the purpose for which video surveillance is being introduced could be achieved in another way that is less intrusive to the privacy and other fundamental rights and freedoms of individuals. In doing so, they must take into consideration, inter alia, the categories of individuals who would be covered by the surveillance. If they decide to introduce video surveillance, they must in any case ensure that all conditions for the lawfulness of personal-data processing through such a system are met. We emphasise that responsibility for ensuring that processing is compliant with the Law always lies with the Controller, who must be able to demonstrate that the processing is carried out in accordance with the Law, including the practical observance of all processing principles.

When video surveillance in the working environment is concerned, i.e. the processing of employees' personal data by the employer, it should be borne in mind that, pursuant to Article 91 of the Law on Personal Data Protection, the processing of personal data in the field of labour and employment is governed by the provisions of the laws regulating labour and employment and by collective agreements, alongside the application of the provisions of this Law. Accordingly, in such cases of processing, the provisions of the Labour Law and other regulations governing matters of labour and employment in the specific situation apply primarily. However, even when employees' personal data are processed by means of video surveillance or through other systems used to monitor their work, movement, communication, or systems intended to analyse/predict a person's tendencies, reliability or behaviour, it must be borne in mind that employees have the right to privacy in their working environment. In each specific case, the necessity and proportionality of such processing must first be examined, in accordance with Article 5 of the Law.

We also draw attention to the Controller's obligation, established by Article 54 of the Law on Personal Data Protection, whereby, if it is likely that a particular type of processing — especially through the use of new technologies and taking into account the nature, scope, circumstances and purpose of the processing — will result in a high risk to the rights and freedoms of natural persons, the Controller must, before commencing such processing, carry out an assessment of the impact of the intended processing operations on the protection of personal data.

The cases in which the Controller is obliged to conduct a data-protection impact assessment are prescribed by Article 54(4) of the Law, as well as by the Decision on the List of Types of Personal Data Processing for Which a Data-Protection Impact Assessment Must Be Carried Out and an Opinion Requested from the Commissioner for Access to Information of Public Importance and Personal Data Protection ("Official Gazette of the RS", Nos. 45/2019 and 112/2020 – hereinafter: the Decision). Under point 2, sub-points 1) to 9) of the Decision, the cases in which an impact assessment must be carried out are prescribed. However, this list is not exhaustive, since, pursuant to point 3 of the Decision, the obligation to conduct a data-protection impact assessment also exists in other cases where it is likely that a certain type of processing — particularly through the use of new technologies and taking into account the nature and other circumstances of the processing — will result in a high risk to the rights and freedoms of natural persons.

Case Number: 073-14-645/2025-02

3.13. Rights of the individual – data with a designated level of confidentiality

Question: Whether the Commissioner, within the scope of his statutory competences, may remove a confidentiality classification and "disclose" data which, as stated, "became classified by being combined with genuinely classified data", and with which the individual is familiar and which concerns that individual.

The Law on Personal Data Protection also regulates certain rights, such as the right of access to data, rectification and supplementation, erasure of data, etc. These rights belong to the person whose data are being processed and are exercised by submitting a request directly to the Controller. However, these rights are not absolute, and may be restricted in the cases prescribed by the Law, in situations such as the protection of national security, defence, public safety, the prevention, investigation and

detection of criminal offences, the prosecution of perpetrators of criminal offences, or the execution of criminal sanctions, including the prevention of and protection from threats to public safety, etc. (Article 40 of the Law).

First, based on your submission, it cannot be determined which specific data are in question, within which procedure and on what legal basis they are being processed, by which entity or entities, nor for the purpose of exercising which right you seek access to them.

The Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18), the implementation of which falls within the competence of the Commissioner, systematically regulates the principles of personal-data processing, as well as other general rules and certain obligations for Controllers and other entities, whereas the processing of personal data in the relevant fields/activities is regulated by special regulations whose application is overseen by other authorities.

In this regard, we point out that the matter relating to the system for classification and protection of classified information that are of interest to national and public security, defence, internal and foreign affairs of the Republic of Serbia, including access to classified information and the termination of their classified status, as well as other matters relevant to the protection of classified information, is governed by the Law on Classified Information, the implementation of which does not fall within the competence of the Commissioner.

The competences and tasks of the Commissioner in relation to the exercise of the rights of data subjects are established by Article 78(1)(6) of the Law, according to which the Commissioner acts upon complaints submitted by data subjects, that is, in cases where the Controller to whom the data subject has previously submitted a request for the exercise of a specific right fails to act upon the request within the prescribed time limit, or if the individual, after receiving the requested information, considers that the processing of his or her personal data has been carried out contrary to the provisions of that Law.

Case Number: 073-14-1352/2025-02

3.14. Whether the document entitled "Data Protection Policy", adopted at the level of a group of commercial entities, may be regarded as a code of conduct.

Question: Whether the document entitled "Data Protection Policy", which is, as stated, adopted at the level of the group and applied to the entity in Serbia "to the extent that it is not contrary to the provisions of the domestic Law on Personal Data Protection", could be regarded as "a Code

of Conduct which, as such, could be approved by the Commissioner from the standpoint of the domestic Law on Personal Data Protection", as well as what needs to be done in order to "complete that procedure".

The document you have enclosed cannot, as you state, be "considered" a Code of Conduct within the meaning of Article 59 of the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018). A Code of Conduct represents a voluntary self-regulatory mechanism for controllers/processors; therefore, its adoption is provided for in the Law only as an option, not as an obligation. However, if controllers decide to develop a Code of Conduct, it should be borne in mind that, pursuant to Article 59(3) of the Law, a Code of Conduct must include provisions enabling the body referred to in Article 60(1) of the Law to supervise the application of the Code by controllers or processors that have undertaken to apply it, without prejudice to the Commissioner's inspection and other powers under Articles 77 to 79 of the Law.

We take this opportunity to provide you with a more detailed explanation of the concept of a Code of Conduct, and first point out that, pursuant to Article 59(1) of the Law, a Code of Conduct may be developed by associations and other entities representing groups of controllers or processors, for the purpose of ensuring more effective application of the Law, particularly with regard to the following matters:

1) fair and transparent processing;
2) the legitimate interests of the controller, taking into account the circumstances of specific cases;
3) the collection of personal data;
4) the pseudonymisation of personal data;
5) information provided to the public and to data subjects;
6) the exercise of data-subject rights;
7) information provided to minors, their protection, and the manner in which the consent of a parent exercising parental responsibility is obtained;
8) the measures and procedures referred to in Articles 41 and 42 of this Law, as well as measures aimed at ensuring processing security under Article 50 of this Law;
9) notifying the Commissioner of a personal-data breach, as well as informing data subjects of such breaches;
10) the transfer of personal data to other countries or international organisations.
11) the manner of resolving disputes between the controller and the data subject by peaceful means, without prejudice to the data subject's rights under Articles 82 and 84 of this Law.

Furthermore, pursuant to Article 59(4) and (5) of the Law, associations and other entities referred to in paragraph 1 of that Article which intend to develop a Code of Conduct or amend an existing one are required to submit the draft Code or its amendments to the Commissioner for an opinion. The Commissioner shall issue an opinion on whether the draft Code of Conduct or its amendments comply with the provisions of the Law, and if the Commissioner determines that the draft Code contains sufficient safeguards for the protection of personal data, the Code of Conduct or its amendments shall be registered and publicly published on the Commissioner's website.

According to Article 60(1) of the Law, the supervision of the application of a Code of Conduct may be carried out by a legal entity accredited for such supervision in accordance with the law regulating accreditation. Article 60(3) further prescribes that such legal entity may be accredited only if it has:

1) demonstrated to the Commissioner its independence and expertise in relation to the content of the Code;
2) established a procedure for assessing the ability of controllers and processors to apply the Code of Conduct, monitoring their application of the Code, and periodically reviewing its effectiveness;
3) established a procedure and a body for deciding on complaints concerning breaches of the Code of Conduct or its application by controllers or processors, and ensured the transparency of such procedure and body to the public and to data subjects;
4) demonstrated to the Commissioner that no conflict of interest may arise in the exercise of its powers.

Article 60(8) of the Law stipulates that paragraphs 1 to 7 of that Article do not apply to public authorities and to processing carried out by competent authorities for special purposes.

From the cited provisions of the Law, it follows, inter alia, that one of the conditions that must necessarily be fulfilled for the Commissioner to be able to grant approval for a draft Code of Conduct prepared by the entities referred to in Article 59(1) of the Law is that the draft Code contains provisions on the accredited legal entity that will supervise the application of that Code.

In this regard, we emphasise that, under the current statutory framework laid down in Article 60 of the Law, the accreditation of a legal entity for supervising the application of a Code of Conduct is not possible at this time.

Namely, Article 60(1) of the Law stipulates that a legal entity shall be accredited for the supervision of the application of a Code of Conduct in accordance with the law governing accreditation, while paragraph 3 of the same Article prescribes the conditions that a legal entity must fulfil in order to be accredited. Of the four conditions established by the mentioned provisions of the Law, two require that their fulfilment be demonstrated to

the Commissioner, namely: independence and expertise in relation to the content of the Code, and the absence of any conflict of interest in the exercise of the legal entity's powers.

However, under the Law on Accreditation ("Official Gazette of the RS", Nos. 73/2010 and 47/2021), the performance of accreditation activities is entrusted to the Accreditation Body of Serbia (Article 5), while the accreditation procedure is regulated by Articles 14–19 of that Law.

Bearing in mind the aforementioned statutory provisions, it is not possible to interpret unambiguously the intention of the legislator with regard to the authority competent for carrying out the accreditation of a legal entity for supervising the application of a Code of Conduct, nor the course of the accreditation procedure.

At the same time, although Article 60(3) of the Law establishes the conditions a legal entity must meet in order to be accredited, the Law does not prescribe the manner in which compliance with those conditions is to be demonstrated, nor does it grant authority to the Commissioner, or to any other body, to regulate this matter in more detail by means of a subordinate act.

Given that neither the Law on Personal Data Protection nor the Law on Accreditation, to which the Law on Personal Data Protection refers, contains provisions that could be comprehensively applied to the accreditation of a legal entity for supervising the application of a Code of Conduct, and bearing in mind that the shortcomings identified can be remedied only through amendments to the Law on Personal Data Protection, the provisions of that Law relating to Codes of Conduct cannot, for the time being, be applied to associations and other entities representing groups of controllers or processors that do not have the status of a public authority.

Case Number: 073-14-1467/2025-02

3.15. How to regulate mutual relations between participants in processing – transfer of data to another country

Question: A healthcare institution has requested an opinion, stating: "An insurance intermediary registered in the territory of France, with whom we wish to establish business cooperation (we would be in a relationship of Independent Controllers), requires us to sign the Standard Contractual Clauses defined by the European Commission, which… also contain the following provisions relating to the governing law and court… *This Agreement is governed by French law… Should the parties fail to reach such a settlement, the matter will be referred to the Nanterre Commercial Court in France*… All of this is unacceptable to us, bearing in mind that we

provide healthcare services in the territory of the Republic of Serbia and that we are obliged to handle patient data and their medical documentation in accordance with our domestic legislation." In this regard, the following questions were raised: "How should a legal entity from Serbia, which has the status of an independent controller, regulate the processing of personal data with another legal entity, also an independent controller from the EU? Can we consider that France ensures an 'adequate level of protection' so that a contract (SCCs) is not required in this specific case? If we nevertheless conclude a personal-data-processing agreement with a foreign entity, regardless of whether its country is on the adequate-protection list or not, may we/should we insist on stipulating the law of the Republic of Serbia and the court in Belgrade as the competent court, bearing in mind that healthcare services are provided in the territory of the Republic of Serbia?"

Bearing in mind that, in your submission, you stated that the entities involved in the intended processing would be "Independent Controllers", we note that the Standard Contractual Clauses adopted by the Commissioner – the Decision Establishing Standard Contractual Clauses ("Official Gazette of the RS", No. 5/20 of 22 January 2020) – regulate the relationship between a controller and a processor in cases where the controller is obliged to carry out the processing of personal data, including the transfer of personal data to another country, to a part of its territory or to one or more sectors of specific activities in that country, or to an international organisation, in accordance with the Law and other applicable regulations of the Republic of Serbia. Accordingly, the Standard Contractual Clauses adopted by the Commissioner may be applied as a means of ensuring appropriate safeguards for the protection of personal data in the context of a transfer of personal data to another country, to a part of its territory or to one or more sectors of specific activities in that country, or to an international organisation for which the list referred to in Article 64(7) of the Law on Personal Data Protection does not establish an adequate level of protection only when the transfer takes place from a controller to a processor.

First, we note that the Commissioner exercises his competences in accordance with the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18; hereinafter: the Law), and not in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). We therefore provide our response strictly from the standpoint of the competences of the Commissioner as established by the provisions of the Law on Personal Data Protection.

Pursuant to Article 3(3) and (4) of the Law, the Law applies to the processing of personal data carried out by a controller or processor that has its seat, residence or domicile in the territory of the Republic of Serbia, within the scope of activities undertaken on the territory of the Republic of Serbia, regardless of whether the processing operation itself takes place on the territory of the Republic of Serbia. The Law also applies to the processing of personal data of data subjects who have their residence or domicile in the territory of the Republic of Serbia by a controller or processor that does not have its seat, residence or domicile in the territory of the Republic of Serbia, if the processing activities relate to: 1) offering goods or services to the data subject on the territory of the Republic of Serbia, regardless of whether the data subject is required to pay for those goods or services; 2) monitoring the activities of the data subject, insofar as those activities take place on the territory of the Republic of Serbia.

Accordingly, bearing in mind the cited statutory provisions, when the processing of personal data is subject to the Law on Personal Data Protection of the Republic of Serbia, the legal relationship between the entities participating in a particular processing operation must be regulated in accordance with that Law.

Namely, when the participation of several entities is envisaged in a particular processing operation, it is necessary to determine the status of each of them (controller, processor, joint controllers, etc.) with regard to the specific processing, so that the provisions of the Law can be correctly applied and the corresponding obligations prescribed by the Law fulfilled, both for controllers and for other entities. The mutual relations between the participants in the processing must be regulated appropriately, in accordance with the Law, and this represents the duty of every controller.

Additionally, since responsibility for the application of the Law lies with the Controller, every Controller is obliged, before commencing the processing of personal data, to first determine whether the conditions for lawful processing of personal data are met in the specific case. This requires, above all, taking into account the special regulations governing the relevant field/activity, ensuring the existence of an appropriate legal basis within the meaning of Article 12 of the Law, and, in the case of processing special categories of personal data, which include health-related data, ensuring that the processing falls under one of the cases set out in Article 17(2) of the Law. The Controller must also apply the principles of processing, comply with the obligations and rules prescribed by the Law, including providing information to the data subject in accordance with Article 23 of the Law, and must take appropriate protective measures to ensure that processing is carried out in accordance with the Law and that the Controller is able to demonstrate this. This assessment must take into account the nature, scope, circumstances and purpose of the processing, as well as the likelihood and level of risk to the rights and freedoms of natural persons.

We further point out that, if personal data are transferred to other countries or international organisations, such transfers are lawful only if the conditions prescribed in Articles 63–72 of the Law are fulfilled, in addition to the other conditions established by the Law, such as the existence of an appropriate legal basis and purpose of processing, data minimisation, and the provision of adequate personal-data protection, etc.

Article 64(1) of the Law stipulates that the transfer of personal data to another country, to a part of its territory, or to one or more sectors of specific activities in that country, or to an international organisation, may be carried out without prior approval if it has been established that the other country, part of its territory, sector or international organisation ensures an adequate level of personal-data protection. Article 64(2) further provides that an adequate level of personal-data protection is deemed to exist in the member states of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as well as in those countries, parts of their territories, or sectors of specific activities, or in international organisations for which the European Union has determined that an adequate level of protection is ensured.

When transferring personal data to another country, to a part of its territory, or to one or more sectors of specific activities in that country, or to an international organisation for which the list referred to in Article 64(7) of the Law does not establish the existence of an adequate level of protection, the appropriate safeguards for such data may, pursuant to Article 65(2) of the Law, be ensured without a special approval from the Commissioner by using the Standard Contractual Clauses drafted by the Commissioner in accordance with Article 45 of the Law, which comprehensively regulate the legal relationship between the controller and the processor.

This opinion is of a general nature and is provided from the standpoint of personal-data protection. In this regard, we also point out that the Law regulates, in a systematic manner, the principles and other general rules of personal-data processing, while the processing of personal data in the relevant spheres of life is governed by special regulations, the implementation of which does not fall within the competence of the Commissioner.

Questions relating to the content of medical documentation and patients' rights are regulated by healthcare legislation. Thus, the Law on Health Documentation and Records in the Field of Healthcare regulates, inter alia, health documentation and records, the types and content of health documentation and records, the processing of data and the manner of handling data from patients' medical documentation used for data processing, etc. As the Ministry of Health is responsible for overseeing the implementation of this Law and other regulations governing the field of healthcare (the Law on Healthcare, the Law on Patients' Rights, etc.), you may also address that authority.

Finally, we point out that, pursuant to Article 5(2) of the Law, responsibility for compliance lies with the Controller, who must be able to demonstrate that the specific processing is carried out in accordance with the Law.

Case Number: 073-14-1169/2025-02

3.16. Processing of employees' biometric data (fingerprint) when entering business premises – obligation to conduct a data-protection impact assessment

Question: A commercial company is considering processing the biometric data of its employees "by taking employees' fingerprints when they enter the employer's business premises". It therefore asks whether it is necessary "first to carry out a data-protection impact assessment and submit it to the Commissioner for approval, and only thereafter prepare consent for the processing of these biometric data". In this regard, a "confirmation" has been requested from this authority "as to whether this is the correct procedure", having regard, as stated, to point 2 of the Decision on the List of Types of Personal Data Processing for Which a Data-Protection Impact Assessment Must Be Carried Out and an Opinion Requested from the Commissioner for Access to Information of Public Importance and Personal Data Protection ("Official Gazette of the RS", Nos. 45/2019 and 112/2020).

From the standpoint of personal-data protection, we generally note that, when the employer processes employees' personal data for the purpose of exercising rights and obligations arising from employment, the employee's consent would not constitute an appropriate legal basis for processing. Rather, the employer's authority to carry out such processing should primarily derive from the relevant regulations in the field of labour, employment, etc. Furthermore, not all categories of personal data collected and subsequently processed from employees fall under the same legal regime of processing, nor do they entail the same risks for the rights and freedoms of individuals, primarily due to the nature of such data and their differing impact on privacy and other rights and freedoms when processed. It must always be borne in mind that employees have a right to privacy in the workplace; therefore, the employer, as Controller, may not pursue the purpose of processing in a manner that excessively intrudes upon employees' privacy, particularly where other, less intrusive methods of achieving that purpose are available to the employer. The purpose of the processing itself—that is, the reason for collecting certain employee data—must first be clear, specifically defined, justified, and lawful.

In this regard, we first note that the competences of the Commissioner in the field of personal-data protection are established by Articles 77–79 of the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18), pursuant to which the Commissioner is not authorised to take a position on specific cases of personal-data processing outside the appropriate procedures within his competence, in which the authority determines the relevant circumstances and facts of the case (inspection-supervision procedure, procedure upon a data-subject complaint, etc.).

It should also be borne in mind that the Law on Personal Data Protection systematically regulates the principles of personal-data processing, as well as other general rules and obligations, whereas the processing of personal data in the relevant spheres of social life/activities is regulated by special regulations, the implementation of which is overseen by other authorities.

The processing of employees' personal data carried out by an employer for the purpose of exercising rights and fulfilling obligations arising from employment is not regulated by the Law on Personal Data Protection. Rather, Article 91 of that Law prescribes that, in the field of labour and employment, the provisions of the laws governing labour and employment and collective agreements shall apply, alongside the provisions of the Law. Oversight of the correct application of labour regulations falls within the competence of the Ministry of Labour, Employment, Veteran and Social Affairs.

Article 4(1)(15) of the Law defines the term "biometric data", specifying that it means personal data obtained by special technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that person, such as an image of his or her face or his or her dactyloscopic data.

The processing of this type of data is subject to a restrictive regime, bearing in mind that, pursuant to Article 17 of the Law, the processing of biometric data for the purpose of uniquely identifying a person is prohibited, and only as an exception may such processing be permitted, namely in the cases set out in paragraph 2 of the same Article. These include, inter alia, situations in which the processing is necessary for the performance of obligations or the exercise of rights prescribed by law for the controller or the data subject in the field of labour, social insurance and social protection, provided that such processing is prescribed by law or by a collective agreement which lays down appropriate safeguards for the fundamental rights, freedoms and interests of the data subject.

Regarding the obligation to conduct a data-protection impact assessment, such an obligation exists in the cases prescribed by the Law and by the above-mentioned Decision of the Commissioner. One of the processing operations for which an impact assessment must be carried out is the processing of biometric data for the purpose of the unique identification of

employees by the employer, as well as other cases of the employer's processing of employees' personal data through applications or systems used to monitor their work, movement, communication, etc. (point 2, sub-point 7 of the Decision).

Therefore, in the case mentioned, the employer is obliged, before commencing the processing itself, to carry out a data-protection impact assessment, which entails adopting a separate impact-assessment act containing all elements prescribed by the Law, etc. However, conducting a data-protection impact assessment is only one of the Controller's obligations. For any processing the Controller intends to carry out, an appropriate legal basis within the meaning of Article 12 of the Law must first be ensured, as well as fulfilment of one of the conditions under which the processing of special categories of personal data is permitted pursuant to Article 17 of the Law, while also complying with all other processing principles in Article 5 of the Law and the relevant rules and obligations, depending on the facts and circumstances of the specific case. If all the aforementioned conditions are not met, such processing cannot be considered lawful under the Law on Personal Data Protection.

Pursuant to Article 55(1) of the Law, the Controller is obliged to request the Commissioner's opinion before commencing the processing operation if the data-protection impact assessment carried out in accordance with Article 54 of the Law indicates that the intended processing operations will result in a high risk unless measures are taken to reduce that risk – that is, only in cases where, even after the implementation of appropriate measures, the level of risk remains high.

More information on the rights and obligations established by the Law on Personal Data Protection, as well as on various issues and positions of the Commissioner concerning the application of this Law, can be found on the Commissioner's website: www.poverenik.rs, in the "Data Protection" section, where you can also find the Guidelines for Conducting a Data-Protection Impact Assessment.

Case Number: 073-14-1636/2025-02

3.17. Collection of data for statistical purposes

Question: An opinion has been requested regarding the conduct of a survey which, as stated, is being carried out by the Statistical Office of the Republic of Serbia in cooperation with a certain organisation. It is further stated that "personal questions" were asked, and that the individual was

not informed about the survey, its purpose, the legal basis, the manner of processing, or the protection of the data being collected. Therefore, answers have been requested on the following: whether the survey is indeed part of an official statistical research project, who exactly the data controller is, whether the collection of first and last names is lawful in this context, which protection mechanisms and data-subject rights have been applied in this research, etc.

In this regard, we note that Article 92(1) of the Law on Personal Data Protection prescribes that, for processing carried out for the purposes of archiving in the public interest, scientific or historical research, or statistical purposes, appropriate measures to safeguard the rights and freedoms of individuals must be applied as required by the Law. These measures ensure the implementation of technical, organisational and staffing safeguards, in particular to ensure compliance with the principle of data minimisation and may include pseudonymisation where the purpose of the processing can be achieved through that measure. Article 92(2) further provides that, if the purposes referred to in paragraph 1 can be achieved without identifying or without further identifying the data subject, those purposes must be fulfilled in a manner that prevents further identification of that person.

Bearing in mind your questions, we first note that the provisions of the Law on Official Statistics regulate matters relating to the performance of activities concerning the organisation of statistical surveys, the collection, processing and publication of official statistical data, the confidentiality and protection of confidential data, the protection of data providers, the authorisation to collect and verify data, the obligation to inform the reporting unit, cooperation with international statistical organisations, etc. Oversight of the implementation of this Law does not fall within the competence of the Commissioner, but within the competence of the Statistical Office of the Republic of Serbia.

The Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018), which the Commissioner is responsible for implementing, regulates in a systemic manner the principles of personal-data processing, as well as other general rules and certain obligations for controllers and other entities, while the processing of personal data in the relevant fields/activities is regulated by special regulations.

From the standpoint of personal-data protection, we note that, in every processing operation, the Controller is obliged to adhere to the general processing rules and other obligations established by the Law on Personal Data Protection. Specifically, this means that the purpose of the processing must be clearly defined, explicit, justified and lawful; that an appropriate legal basis must exist for the processing; that the processing must be car-

ried out in accordance with the special regulations governing the relevant field; and that the processing must comply with the principles set out in Article 5 of the Law, including the principle of data minimisation, under which only the data that are genuinely necessary to achieve the purpose may be collected and processed.

Pursuant to the principle of "accountability" under Article 5(2) of the Law on Personal Data Protection, responsibility for the correct application of the Law lies with the Controller, who must be able to demonstrate compliance with the obligations prescribed by the Law in relation to the processing of personal data.

In addition to the above-mentioned obligations of the Controller, the Law on Personal Data Protection regulates certain rights of individuals, such as the right of access, the right to rectification and supplementation, the right to erasure of personal data, etc. These rights belong to the data subject whose data are being processed and are exercised by submitting a request to the Controller, i.e. the entity that is processing the individual's personal data in the specific case. The Commissioner acts upon complaints submitted by data subjects, namely when the Controller to whom the individual has previously submitted a request for the exercise of a particular right fails to act upon that request, or if the individual, after receiving a response, considers that the processing has been carried out contrary to the provisions of the Law.

However, we note that the rights of individuals regulated by the Law on Personal Data Protection are not absolute, as they may, in exceptional cases prescribed by the Law, be restricted.

We further note that Article 92(3) of the Law on Personal Data Protection provides that the provisions on the rights of data subjects under Articles 26, 29, 31 and 37 of the Law shall not apply where processing is carried out for scientific or historical research purposes or for statistical purposes, if their application is necessary to achieve those purposes or if the application of those provisions would prevent or significantly impede the achievement of those purposes, provided that the measures referred to in paragraphs 1 and 2 of that Article are applied.

Case Number: 073-14-1552/2025-02

3.18. Possibility of identifying the perpetrator of an offence by showing a photograph to the injured party

Question: A public authority has requested an opinion, stating that inspectors, based on the data submitted with a report, have the possibility to, for the purpose of identifying the perpetrator of an offence, show a photograph from the database to the injured party "for identification and

further conduct of the procedure". The submission to the Commissioner further quotes the provisions of Articles 9, 12 and 19 of the Law on Personal Data Protection, and, given that conduct contrary to the Law on Passenger Transport in Road Traffic "constitutes a punishable act" for which a misdemeanour sanction is prescribed and imposed by the Misdemeanour Court, in proceedings initiated upon a request submitted by a road-traffic inspector, the following question has been raised: "Is the identification of the perpetrator of an offence by showing a photograph to the injured party, without the prior consent of the data subject, in accordance with the provisions of the Law on Personal Data Protection, particularly bearing in mind that this concerns processing necessary for the performance of tasks carried out in the public interest or in the exercise of the controller's statutory powers, pursuant to Article 12(1)(5) of the said Law?"

Accordingly, even in the situation you describe consent for the processing of personal data would not constitute an appropriate legal basis. Rather, as already noted, inspectors may derive their authority to process such data solely from the relevant special regulations. Furthermore, the processing of personal data itself must be carried out in the manner and within the limits of the powers established by those special regulations, which also applies to the possibility of identifying a driver in the manner described. Thus, it must be determined whether such a possibility is provided for at all by the specific laws governing the powers and procedures of inspectors; if it is not, such processing cannot be considered permissible. Likewise, obtaining, for example, the individual's consent could not be viewed as an appropriate legal basis for the processing, because consent, pursuant to Article 15 of the Law, must meet certain criteria to be regarded as a valid legal ground — such as voluntariness, absence of coercion, the right to withdraw consent at any time, etc. — all of which make it inapplicable to processing carried out by public authorities in the exercise of their statutory powers.

Accordingly, we hereby provide the following general guidance.

The conditions and manner of performing public passenger transport by road, as well as the inspection oversight of the implementation of that Law, are regulated by the Law on Passenger Transport in Road Traffic. This Law also regulates the rights and duties of inspectors when conducting inspection oversight, as well as their powers.

The Law on Personal Data Protection regulates, in a systemic manner, the principles of personal-data processing and other relevant rules and obligations, making a distinction between the general regime of personal-data processing and the special regime applicable to processing carried out by competent authorities for the purposes of preventing, investigating

and detecting criminal offences, prosecuting offenders or enforcing criminal sanctions, including preventing and protecting against threats to public and national security.

The term "competent authorities" is defined in Article 4(26) of the Law, pursuant to which the category of competent authorities, within the meaning of that Law, includes only those public authorities responsible for the prevention, investigation and detection of criminal offences, as well as the prosecution of offenders or the enforcement of criminal sanctions, including the protection of and prevention against threats to public and national security. Therefore, under the currently applicable provisions of the Law, processing carried out for the purpose of preventing misdemeanours or detecting them, etc., is not considered to fall under the special processing regime; instead, the provisions of the Law governing the general processing regime apply to such processing.

The Law on Personal Data Protection provides six possible legal bases for processing (Article 12). When public authorities act as Controllers, their authority to process personal data within the scope of their competences must primarily derive from the provisions of special laws. Accordingly, public authorities may collect and further process only those personal data that are necessary for the performance of their statutory powers.

In addition to ensuring an appropriate legal basis for the processing, it is necessary that the processing be carried out in accordance with all the processing principles set out in Article 5 of the Law ("lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation", "integrity and confidentiality"). In this regard, and bearing in mind your statements concerning the presentation to the injured party of a photograph of "the taxi driver who performed the ride at the critical moment" for the purpose of "identification and further conduct of the procedure", it cannot be concluded that such an approach would result in the processing of reliable, i.e. accurate, personal data concerning the identity of the driver. Accuracy is, of course, one of the obligations of the Controller under the above-mentioned principle of accuracy.

At this point, we also remind you of the Controller's obligation to involve, in a timely and appropriate manner, the Data Protection Officer designated by the Controller in all matters relating to personal-data protection (Article 57). We further note that this person is, among other things, obliged to inform and advise the Controller, as well as the employees who carry out processing operations, of their statutory obligations concerning personal-data protection (Article 58).

Case Number: 073-14-2071/2025-02

3.19. Use of photographs of pupils that are available on the school's website

Question: An opinion has been requested regarding the following: "For the recording of an educational film with which I am being nominated for a global teachers' competition… I wished to use photographs of activities with pupils that I carried out at the school… the photographs are available on the school's website and the school's Facebook page." It is further stated that parents signed consent for those photographs to be posted, and the question posed is: "May I use those photographs for the recording of an educational film, or do I need additional consent for them, given that they are publicly available?"

When a Controller has processed personal data by making them publicly available for specific purposes, it is necessary to take into account the principle of "purpose limitation" — namely, that personal data may not be further processed in a manner that is incompatible with those purposes, i.e. for a purpose different from the one for which the data were originally processed.

We first note that, based on your submission, it cannot be determined in what capacity you would be participating in the competition in question — that is, whether independently or on behalf of the school in which you are employed — nor, consequently, what your status would be in relation to the intended processing.

The Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018), which the Commissioner is competent to implement, systemically regulates the principles of personal-data processing, as well as other general rules and obligations for controllers and other entities, while the processing of personal data within the relevant areas of social life is governed by special regulations. In this respect, it is therefore necessary to take into account the relevant provisions of such special laws.

In that regard, we note that the performance of secondary-education activities, the manner and conditions for carrying out those activities, the organisation and oversight of the work of educational institutions, as well as other matters of importance for secondary education, are regulated by the provisions of the Law on Secondary Education, the Law on the Foundations of the Education System, and other relevant regulations. As the Commissioner is not competent to provide opinions on the application of these laws, you may contact the Ministry of Education for guidance on their application.

From the standpoint of personal-data protection, we provide the following general guidance:

Article 12 of the Law on Personal Data Protection sets out six possible legal bases for the processing of personal data, namely: 1) the data subject's consent to the processing; 2) performance of a contract concluded with the data subject or taking steps at the request of the data subject prior to the conclusion of a contract; 3) compliance with the Controller's legal obligations; 4) protection of the vital interests of the data subject or of another natural person; 5) performance of tasks carried out in the public interest or in the exercise of the Controller's statutory powers; and 6) the pursuit of the legitimate interests of the Controller or of a third party.

Before the processing of certain personal data may begin, it is necessary first to determine the purpose of the processing, which must be clearly defined, explicit, justified and lawful. Personal data may not be further processed in a manner incompatible with that purpose ("purpose limitation" principle). It is also necessary to ensure that an appropriate legal basis is in place in accordance with Article 12 of the Law on Personal Data Protection, and that the processing is carried out in compliance with the other processing principles set out in Article 5 of the Law, as well as with the other relevant rules and obligations prescribed by the Law, depending on the circumstances of the particular case.

With regard to the data subject's consent as one of the possible legal bases, we note that Article 4(12) of the Law on Personal Data Protection defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which that person, by a statement or by a clear affirmative action, gives consent to the processing of personal data relating to him or her. When the processing concerns a child's personal data, consent must be given by the child's legal representative in accordance with the regulations governing the representation of minors.

Article 15 of the Law on Personal Data Protection prescribes certain conditions that must be met in order for processing based on consent to be considered lawful. Among other things, these include the following: the Controller must be able to demonstrate that the individual has consented to the processing of his or her personal data; if consent is given within a written declaration that also concerns other matters, the request for consent must be presented in a manner that clearly distinguishes it from those other matters, in an intelligible and easily accessible form, and using clear and plain language. The data subject must have the right to withdraw consent at any time; the withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal; prior to giving consent, the data subject must be informed of the right to withdraw consent and of the effects of withdrawal; the withdrawal of consent must be as simple as giving it; and so on.

When assessing whether consent for the processing of personal data has been freely given, particular attention must be paid to whether the per-

formance of a contract, including the provision of services, is being made conditional on the giving of consent that is not necessary for its performance (Article 15(4) of the Law).

In line with the above, we note that every Controller intending to carry out the processing of personal data is obliged to ensure an appropriate legal basis for the processing that is planned.

In that regard, we emphasise that consent for the processing of personal data, once given by an individual to a particular Controller, may constitute a legal basis for the specific processing only for that Controller, and such consent cannot be regarded as a valid legal basis for the processing of personal data by another Controller. Therefore, consent as a legal basis for processing personal data under the Law on Personal Data Protection cannot be transferred, assigned or "passed on" to another Controller, nor can it be obtained or taken over from another Controller.

In accordance with Article 5(2) of the Law, responsibility for compliance lies with the Controller. Therefore, it is the Controller who must be able to demonstrate compliance with the obligations prescribed by the Law in relation to the processing of personal data, which, among other things, includes ensuring an appropriate legal basis for the processing of personal data.

Case Number: 073-14-1625/2025-02

3.20. Collection of data for the purposes of the Commission for Establishing Facts on the Status of Newborn Children Suspected of Having Gone Missing from Maternity Hospitals in the Republic of Serbia – Commissioner's consent

Question: An opinion has been requested concerning the request of the Commission for Establishing Facts on the Status of Newborn Children Suspected of Having Gone Missing from Maternity Hospitals in the Republic of Serbia, whereby the Commission asks the Ministry "to collect from all centres for social work data on adopted children from 1952 to the present day". In this regard, the question has been raised as to whether there is a legal basis for the Ministry "to request the said data from centres for social work, to process them, and to submit them to the Commission", bearing in mind that, as further stated, the "Unified Personal Register of Adoptions has been kept within the ministry responsible for family protection since 2006, that the Ministry does not possess data on adoptions for the period from 1952 to 2006, and that data on adoptions constitute official secrecy pursuant to Article 323 of the Family Law…".

In this regard, we note that, pursuant to Article 29(4) of the Law on Establishing Facts on the Status of Newborn Children Suspected of Having Gone Missing from Maternity Hospitals in the Republic of Serbia ("Official Gazette of the RS", No. 18/2020), the Commission may process personal data only with the consent of the Commissioner for Information of Public Importance and Personal Data Protection, who is obliged to decide on the Commission's request within five days from the date of its receipt. However, since Article 29(2) of the same Law prescribes that the task of the Commission is to collect and process all facts and data held by the authorities and other entities specified in that provision, this means that the Commission has the right to request the necessary data from each centre for social work individually, but not to request the Ministry to collect those data on its behalf. If the data are not in the possession of the Ministry, the Ministry has no obligation to collect data in order to comply with the Commission's request.

In this regard, we inform you of the following.

We first note that the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/2018), which the Commissioner is responsible for implementing, systemically regulates the principles of personal data processing, as well as other general rules and certain obligations, while the processing of personal data in the respective fields/activities is governed by special regulations, the implementation of which falls under the competence of other authorities.

From the standpoint of the Commissioner's competence in applying the Law on Personal Data Protection, we note that the disclosure of personal data — whether by submitting them or in any other way making them available — unquestionably constitutes a processing operation within the meaning of Article 4(3) of the Law, and that certain conditions must therefore be met in order for such disclosure to be lawful.

Specifically, this means that the purpose of the processing must first be clearly defined, justified and lawful. The processing must also be necessary — that is, genuinely required to achieve that purpose. Furthermore, there must be an appropriate legal basis for the processing within the meaning of Article 12 of the Law, and the processing must comply with the special regulations applicable in the relevant field. In addition, all processing must be carried out in accordance with the processing principles set out in Article 5 of the Law, including the principle of data minimisation, as well as the other rules and obligations established by the Law.

If all of the above conditions are not met, the processing cannot be regarded as lawful from the perspective of the Law on Personal Data Protection.

We emphasise that special regulations governing a particular field play a crucial role: Controllers must always ensure that the processing they un-

dertake is, first and foremost, aligned with those special regulations — that is, with the laws and other rules governing the performance of the activity falling within the competence of the authority as Controller (for example, regulations in the areas of social or family-law protection, etc.), as well as with any other special regulations that the Controller is obliged to apply in the specific case.

In accordance with the principle of "accountability" under Article 5(2) of the Law, it is the Controller who must, taking into account all the circumstances of the specific case, determine whether all of the above-mentioned conditions for the intended processing have been met. The Commissioner would adopt a position only within the framework of proceedings initiated and conducted in accordance with the Commissioner's statutory powers, and on the basis of all the facts established in those proceedings. Therefore, outside the context of such proceedings, the Commissioner cannot issue instructions for action, as doing so would prejudge the Commissioner's decision in any potential procedure within his competence.

We also take this opportunity to remind you of the obligation of all Controllers who have appointed a Data Protection Officer to involve that officer, in a timely and appropriate manner, in all matters relating to personal-data protection. One of the tasks of the Data Protection Officer is to inform and advise the Controller, as well as the employees carrying out processing operations, about their statutory obligations in connection with personal-data protection.

Case Number: 073-14-1472/2025-02

3.21. Is the building manager allowed to publish the flat number and the amount of outstanding debt?

Question: An opinion has been requested regarding the following: Is the building manager allowed to publish "the flat number and the amount of that flat's outstanding debt to the building, without the first and last name of the flat owner"?

Thus, any piece of information — including, for example, a flat number — constitutes personal data within the meaning of the cited provision of the Law if, directly or indirectly and in combination with other information, it renders the identity of a natural person determined or determinable. This must be borne in mind in every individual case, and the processing of such data is subject to the principles and rules of processing prescribed by the Law on Personal Data Protection.

In this regard, we inform you of the following.

We first note that matters concerning building management, the rights and obligations of the building manager, and other issues relevant to housing policy are regulated by the Law on Housing and Building Maintenance, the implementation of which falls under the competence of the Ministry of Construction, Transport and Infrastructure. Therefore, for an opinion on the application of that regulation, you may contact the competent ministry.

The Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18), which the Commissioner is responsible for implementing, systemically regulates the principles of personal-data processing and other rules and obligations for controllers and other entities involved in processing. However, the processing of personal data in specific fields or activities is regulated by special laws, the application of which is overseen by other authorities.

From the standpoint of applying the Law on Personal Data Protection, we point out that the concept of personal data is defined in Article 4, item 1) of the Law, which stipulates that personal data are any data relating to a natural person whose identity is determined or determinable, directly or indirectly, particularly on the basis of an identity marker such as a name or identification number, location data, identifiers in electronic communications networks, or one or more characteristics of that person's physical, physiological, genetic, mental, economic, cultural or social identity.

Since the disclosure or any other form of making personal data available constitutes processing of personal data within the meaning of Article 4, item 3) of the Law, we underline that, for personal-data processing to be lawful, it is first necessary to ensure that such processing is in accordance with the special regulations governing the relevant field or activity. Furthermore, the purpose of the processing must be specifically defined, explicit, justified and lawful; an appropriate legal basis must exist for the intended processing within the meaning of Article 12 of the Law; and the processing must be carried out in accordance with the principles of processing laid down in Article 5 of the Law (including the principle of data minimisation and the principle of integrity and confidentiality, which requires that personal data be processed in a manner that ensures appropriate protection, including protection against unauthorised or unlawful processing, through the application of appropriate safeguards), as well as all other applicable rules and obligations established by the Law, depending on the circumstances of each individual case.

Personal-data processing that lacks an appropriate legal basis or is carried out contrary to the prescribed processing principles would not be compliant with the Law.

Given that, pursuant to the accountability principle under Article 5, paragraph 2 of the Law, the controller is responsible for the proper application of the Law, it is the controller who must decide whether, in a particular

case, the conditions for lawful processing of personal data have been met, taking into account, above all, the special regulations governing the specific type of processing. The controller is also obliged, when carrying out the processing, to adhere to all processing principles and other obligations prescribed by the Law and must be able to demonstrate the application of those principles.

Case Number: 073-14-2148/2025-02

3.22. Deletion of an "online" account and withdrawal of consent for processing

Question: An individual sought an opinion, stating that they had created an "online account", that they "immediately afterwards" wished to delete it, that an identity card had been required to open the account, that they were informed that it was not possible to delete the account, and that they continue to receive "promotional messages and emails, even though I have repeatedly asked to be removed from the mailing list". The following question was therefore raised: "Is it really possible that I cannot withdraw my consent for the processing of my personal data and that I cannot request that all my personal data be deleted from their database? As well as that I have no right to deletion of the created account?", noting that the individual received a response stating that the account can only be "deactivated", but that "this is not the same as withdrawing consent for the processing of my personal data…".

With regard to consent as one of the six possible legal bases for the processing of personal data, we note that this legal basis is regulated by Article 15 of the Law, pursuant to which the data subject has the right to withdraw consent at any time (Article 15, paragraph 3 of the Law).

In this regard, as it cannot be determined from your notice to which type of "online account" your enquiry relates, and from the perspective of the Commissioner's competence, we hereby inform you as follows.

First, we note that the right to the protection of natural persons with regard to the processing of personal data is governed by the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18).

This Law regulates, in a systematic manner, the principles of personal data processing, as well as other rules and obligations applicable to controllers and other entities participating in processing, while the processing of personal data in specific areas/activities is regulated by special regulations, the application of which is overseen by other competent authorities.

From the perspective of the application of the Law on Personal Data Protection, we note that, for the lawful processing of personal data, the controller is first required to ensure that such processing is carried out in accordance with the special regulations governing the relevant area/activity, that an appropriate legal basis for the intended processing exists within the meaning of Article 12 of the Law, and that the processing is carried out in accordance with the processing principles laid down in Article 5 of the Law, as well as other applicable rules and obligations prescribed by the Law, depending on the circumstances of each individual case.

The Law on Personal Data Protection also regulates the rights of data subjects whose personal data are processed, such as the right of access, rectification and completion, erasure, and other rights.

The right to the erasure of personal data is prescribed by Article 30 of the Law. Pursuant to paragraph 1 of this Article, the data subject has the right to have his or her personal data erased by the controller. Paragraph 2 of the same Article stipulates that the controller is obliged to erase the data referred to in paragraph 1 of this Article without undue delay in the following cases: 1) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed; 2) the data subject has withdrawn consent on which the processing was based, in accordance with Article 12, paragraph 1, item 1) or Article 17, paragraph 2, item 1) of this Law, and there is no other legal basis for the processing; 3) the data subject has lodged an objection to the processing in accordance with: a) Article 37, paragraph 1 of this Law, and there are no overriding legitimate grounds for the processing which override the interests, rights or freedoms of the data subject; b) Article 37, paragraph 2 of this Law; 4) the personal data have been processed unlawfully; 4) the personal data must be erased in order to comply with a legal obligation of the controller; 6) the personal data were collected in connection with the use of information society services referred to in Article 16, paragraph 1 of this Law.

However, we note that the right to the erasure of personal data is not an absolute right. Article 30, paragraph 5 of the Law provides that paragraphs 1 to 3 of this Article shall not apply to the extent that processing is necessary for: 1) exercising the right to freedom of expression and information; 2) compliance with a legal obligation of the controller requiring the processing, or the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; 3) reasons of public interest in the area of public health, in accordance with Article 17, paragraph 2, items 8) and 9) of this Law; 4) archiving purposes in the public interest, scientific or historical research purposes, or statistical pur-

poses in accordance with Article 92, paragraph 1 of this Law, where it can reasonably be expected that the exercise of the rights referred to in paragraphs 1 and 2 of this Article would render impossible or seriously impair the achievement of the objectives of such processing; 5) the establishment, exercise or defence of legal claims.

The data subject submits a request for the exercise of any of the above rights, including the right to the erasure of personal data, directly to the controller, i.e. the entity processing his or her personal data. Pursuant to Article 21, paragraph 3 of the Law, the controller is obliged to inform the data subject of the action taken in response to the request without delay and, in any event, no later than 30 days from the date of receipt of the request. This period may be extended by a further 60 days where necessary, taking into account the complexity and number of requests. The controller must inform the data subject of any such extension and the reasons for it within 30 days of receipt of the request.

Furthermore, pursuant to Article 21, paragraph 4 of the Law, where the controller fails to act upon a request submitted by the data subject, the controller is obliged to inform the data subject of the reasons for not taking action without delay and, in any event, no later than 30 days from the date of receipt of the request, as well as to inform the data subject of the right to lodge a complaint with the Commissioner or to bring an action before a court.

If the controller fails to act upon the submitted request, or if, after receiving the controller's response, the data subject considers that the processing of his or her personal data is carried out contrary to the provisions of the Law, the data subject has the right to lodge a complaint with the Commissioner in accordance with Article 82 of the Law, and may also seek appropriate judicial protection by filing a claim with the competent higher court, pursuant to Article 84 of the Law.

Having regard to all of the above, we point out that the Law prescribes situations in which the controller will not comply with a data subject's request to exercise the right to erasure of personal data, such as, for example, where the data subject has withdrawn consent on which the processing is based, but another legal basis for the processing exists as prescribed by Article 12 of the Law, and other such cases. The controller is obliged to assess these circumstances in each individual case.

Case Number: 073-14-2204/2025-02

3.23. Provision of electronic access to medical test results

Question: A private healthcare institution has requested an opinion, stating that, since it issues "test results" to patients, there is an option it could introduce whereby "on a separate (secured) server we could enable patients, by logging in, to access their results. The patient would receive a password and login credentials, which only that patient would see and be able to use to access the results." In this context, the question has been raised as to whether explicit written consent from the patient is required, "or whether we, as a healthcare institution, may enable this, leaving it to the patient to decide whether to use such facilities." It is also noted that the "results" would contain the patient's first and last name, "while the server login credentials, i.e. the username and password, would be generated as unique, non-repeating numbers.."

We note that, in accordance with the principle of integrity and confidentiality set out in Article 5, paragraph 1, item 6) of the Law, every controller is required to implement appropriate technical, organisational and staffing measures in order to ensure that the processing of personal data is carried out in compliance with the Law and to be able to demonstrate such compliance. In doing so, the controller must take into account the nature, scope, context and purposes of the processing, as well as the likelihood and severity of the risks to the rights and freedoms of natural persons, with a view to achieving an appropriate level of security in relation to the risk. This includes, in particular, consideration of the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that have been transmitted, stored or otherwise processed (Articles 41, 42 and 50 of the Law). Furthermore, every controller is obliged, when carrying out processing, to comply with all other processing principles laid down in Article 5 of the Law, as well as with the relevant obligations of controllers established by the Law.

The above is particularly relevant in cases where access to data is enabled by electronic means, i.e. in an "online" environment, especially where the data concerned relate to an individual's health. Such data fall within the category of special categories of personal data under Article 17, paragraph 1 of the Law and, given their sensitive nature, require particular caution in handling, as well as the implementation of appropriate measures to protect against unauthorised access to and misuse of such data.

In this regard, we inform you as follows.

First, we note that it cannot be determined from your submission whether, in the specific case, this concerns the exercise of certain patients'

rights, and if so, which specific rights, i.e. pursuant to which regulations. It is also unclear in what specific manner, i.e. through which information systems, the patient would access their "results", and whether this would involve the use of existing information systems or the introduction of new ones, as well as whether the described practice would, in general, be in compliance with the special regulations governing the keeping of medical records and the handling thereof. Furthermore, it is unclear for which specific action or activity an "explicit written consent of the patient" would potentially be required, or whether this refers to consent for the processing of personal data. Nor can it be determined from your submission for what purpose the data enabling "online" access to results (username and password) would be provided to the patient, if such data were to be provided "at the end of the results", as indicated in your submission.

In this regard, given that matters relating to medical documentation and records in the field of healthcare — including the types and content of medical documentation and records, the manner and procedure for their keeping, the persons authorised to keep medical documentation and enter data, the processing of data, the manner of handling data from patients' medical records used for data processing, ensuring data quality, protection and retention, as well as the possibility for patients to access their own medical documentation — are regulated by special legislation governing the relevant field, such as the Law on Healthcare Documentation and Records and other related regulations, and bearing in mind that supervision over the implementation of that Law is exercised by the Ministry of Health, you may contact that Ministry regarding questions relating to its application.

We take this opportunity, from the perspective of the application of the Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18), to point out that, for the processing of personal data to be lawful, the controller is required, first and foremost, to ensure that such processing is carried out in compliance with the special regulations governing the relevant area or activity.

Furthermore, controllers who have appointed a Data Protection Officer in accordance with the provisions of Article 56 of the Law are obliged to involve that person, in a timely and appropriate manner, in all matters relating to the protection of personal data. The Data Protection Officer appointed by the controller is, inter alia, obliged to inform and provide advice to the controller, as well as to employees who carry out processing activities, on their statutory obligations relating to the protection of personal data, in accordance with Article 58, paragraph 1, item 1) of the Law.

As, pursuant to the principle of accountability set out in Article 5, paragraph 2 of the Law, responsibility for the proper application of the Law rests with the controller, it is the controller who decides whether, in a par-

ticular case, the conditions for the lawful processing of personal data are fulfilled, taking into account, first and foremost, the special regulations governing the processing in question. The Commissioner may adopt a position on individual cases of personal data processing only within the framework of proceedings conducted in accordance with his statutory powers (inspection proceedings, proceedings upon a complaint, or other appropriate proceedings within his competence), and on the basis of all the facts and circumstances established in those proceedings.

Case Number: 073-14-2036/2025-02

3.24. Prior opinion of the Commissioner regarding the intention to introduce "GPS tracking of official vehicles"

A commercial company approached the Commissioner and submitted, as an annex, an "Impact Assessment on the Protection of Personal Data (in relation to the processing of data through GPS tracking of official vehicles)", for the purpose of obtaining the opinion of this authority.

FROM THE COMMISSIONER'S ACT

Pursuant to Article 54, paragraph 1 of the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia", No. 87/18 – hereinafter: the Law), a data controller is obliged, where it is likely that a type of processing, in particular through the use of new technologies and taking into account the nature, scope, context and purposes of the processing, will result in a high risk to the rights and freedoms of natural persons, to carry out, prior to commencing the processing of personal data, an assessment of the impact of the envisaged processing operations on the protection of personal data.

The cases in which a controller is required to carry out a data protection impact assessment are prescribed by Article 54, paragraph 4 of the Law and by the Decision on the List of Types of Personal Data Processing Operations for Which a Data Protection Impact Assessment Must Be Carried Out and an Opinion of the Commissioner for Information of Public Importance and Personal Data Protection Must Be Sought ("Official Gazette of the Republic of Serbia", Nos. 45/2019 and 112/2020).

Article 54, paragraph 6 of the Law prescribes the minimum content of a data protection impact assessment and provides that the assessment must, at a minimum, include: a comprehensive description of the envisaged processing operations and the purposes of the processing, including a description of the legitimate interests of the controller, where such interests exist; an assessment of the necessity and proportionality of the processing

operations in relation to the purposes of the processing; an assessment of the risks to the rights and freedoms of the data subjects; a description of the measures envisaged to address the identified risks, including safeguards, as well as technical, organisational and staffing measures aimed at protecting personal data and ensuring evidence of compliance with the provisions of this Law, taking into account the rights and legitimate interests of the data subjects and other persons.

Article 55, paragraph 1 of the Law provides that, where a data protection impact assessment carried out in accordance with Article 54 of the Law indicates that the envisaged processing operations would result in a high risk in the absence of measures taken to mitigate the risk, the controller is obliged to seek the opinion of the Commissioner prior to commencing the processing operations.

Paragraph 7 of the same Article of the Law prescribes the obligation of the controller, when submitting a request for an opinion, to provide the Commissioner with information on: 1) the responsibilities of the controller and, where applicable, of joint controllers and processors involved in the processing, in particular where the processing is carried out within a group of undertakings; 2) the purposes and methods of the envisaged processing; 3) the technical, organisational and staffing measures, as well as the safeguards for protecting the rights and freedoms of the data subjects in accordance with this Law; 4) the contact details of the data protection officer, if one has been appointed; 5) the data protection impact assessment referred to in Article 54 of the Law; and 6) any other information requested by the Commissioner.

Responsibility for acting in accordance with the provisions of the Law lies with the controller. In this regard, we emphasise that the Commissioner is not obliged to issue an opinion where the conducted data protection impact assessment indicates that the envisaged processing operations will result in a low level of risk to the protection of personal data, or that, following the implementation of measures, the level of risk will not be high. Namely, as already stated, pursuant to Article 55, paragraph 1 of the Law, the obligation to submit a request for a prior opinion of the Commissioner applies only in situations where the data protection impact assessment indicates that the envisaged processing operations would result in a high risk if measures to mitigate the risk are not taken.

Having regard to the foregoing, we first note that the submitted document is not signed and that it is therefore unclear whether it constitutes an act of the controller or an unofficial, draft version of the document. Namely, under the Law, a data protection impact assessment is adopted by the controller, and as such the relevant document must be signed by the person authorised to represent the controller.

However, the Commissioner has reviewed the content of the submitted document and, in general terms, points out the following.

In Section 1 of the submitted Act, entitled "Introductory Provisions", it is stated that "this document constitutes a Data Protection Impact Assessment in accordance with Article 54 of the Law on Personal Data Protection … as well as Article 35 of the General Data Protection Regulation (GDPR …)". In this regard, we point out that the obligation to carry out a data protection impact assessment arises from the Law on Personal Data Protection and that such an assessment is conducted in accordance with the provisions of that Law, and not in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Furthermore, in Section 3, "Description of the Processing", it is stated that the purpose of the processing is "tracking the movement of company vehicles using GPS technology for the purpose of: efficient planning and control of the use of company vehicles, ensuring the safety of employees and property, determining responsibilities arising from the employment relationship, recording actual routes travelled for the purposes of cost calculation and working time control".

From the above, it follows that the purpose of the processing of personal data is not clearly defined, but rather that various objectives relating to the use of a particular technological solution are conflated with the purpose of the processing of personal data carried out through that solution.

In this regard, we note that, pursuant to Article 5, paragraph 1, point 2) of the Law, the purpose of processing must be specific, explicit, legitimate and lawful. Accordingly, the purpose of the processing must be defined in accordance with the Law and clearly distinguished from the objective(s) of specific activities.

With regard to the statement in the same section of the submitted Act that "the categories of data subjects are: employees to whom vehicles for official use have been assigned", we note that the controller has not specifically identified which personal data of employees (natural persons) it intends to process. Furthermore, when processing employees' personal data, the controller must take due account of the data minimisation principle set out in Article 5, paragraph 1, point 3) of the Law, which provides that personal data must be adequate, relevant and limited to what is necessary in relation to the purpose of the processing.

In addition, it is necessary to further specify the statements made in the section "Scope of Processing", in particular what is meant by "time stamps (date and time)" and by "vehicle and driver identifier", in terms of the type of personal data and the scope of the processing. It is unclear over what period of time the movement of vehicles and drivers will be monitored, whether monitoring will take place exclusively during working hours

or also outside working hours, whether monitoring is envisaged throughout the entire working time or only during the performance of specific activities, and similar issues.

In Section 4, "Legal Basis for Processing", it is stated, inter alia, that the processing is based "on Article 12, paragraph 1, point 6) of the Law – where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party."

Having regard to the quoted statement, we note that legitimate interest is indeed one of the six possible legal bases for the processing of personal data; however, its application requires that the conditions prescribed by the Law be met, namely: the existence of a specific legitimate interest of the controller or a third party; the necessity of the processing; and the overriding nature of the legitimate interest over the interests or fundamental rights and freedoms of the data subject. Accordingly, taking into account all relevant aspects of the envisaged processing, including the specific regulations governing such processing (e.g. regulations in the field of employment and labour law, etc.), it is first necessary to determine whether legitimate interest constitutes an appropriate legal basis for the intended processing, i.e. whether all the conditions for its application under Article 12, paragraph 1, point 6) of the Law on Personal Data Protection are fulfilled. However, this cannot be established on the basis of the submitted Data Protection Impact Assessment. Further information on legitimate interest as a legal basis for the processing of personal data is available on the website of the Commissioner at www.poverenik.rs, under "Personal Data Protection" – "Legitimate Interest".

In the submitted document, Section 5, "Assessment of Necessity and Proportionality", states that "the processing is necessary for the planning and control of the use of official vehicles, the prevention of misuse (e.g. use for private purposes contrary to internal rules), cost control and business rationalisation", and that "the processing is proportionate because: the data are not processed for private purposes, and employees have been informed in advance of the purpose and manner of processing (transparency)". In this regard, we note that, as concerns the arguments put forward to substantiate the necessity of the processing, we are of the view that they are not sufficient to conclude that the processing of personal data could be regarded as genuinely necessary and indispensable for achieving the stated purpose. This is primarily because the above statements of the controller are not substantiated: it is not explained how such conclusions were reached, nor are reasons provided as to why less intrusive means of processing would not enable the purpose to be achieved. By way of example, the document does not specify how the controller currently monitors the movement of official vehicles, for what specific reasons such a method of monitor-

ing is considered insufficient to achieve the purpose of the processing, which measures the controller has taken to remedy any shortcomings of the existing method of monitoring the movement of official vehicles, or which other reasons would unequivocally demonstrate the necessity of the envisaged processing. All of the above must be documented by the controller, in accordance with the obligation arising from Article 5, paragraph 2 of the Law

In Section 6 of the submitted Act, "Identification and Assessment of Risks", a tabular overview is provided in which the "identified risks" and their "assessment" are presented and classified as high/medium. The table also contains a "Description of the risk"; however, neither the specific sources of risk nor the potential consequences that could arise are specified or described. Consequently, it is not possible to assess whether the "Proposed measures" for risk mitigation are sufficient and appropriate.

Namely, in order to assess the level of risk, it is necessary to take into account both the likelihood/probability of harm occurring to the rights and freedoms of the data subjects and the severity of the potential harm, i.e. the extent of the impact that the harm would have on the rights and freedoms of the individuals whose personal data are being processed (e.g. negligible, medium or high). On the basis of these two parameters, the level of risk should then be determined, followed by the identification of appropriate measures to mitigate those risks.

We further note that risks to the rights and freedoms of data subjects should not be limited solely to events that have the potential to affect the right to the protection of personal data, but should also encompass other events that may arise in the course of processing and which may lead to the loss or impairment of any human right or freedom of the individual, such as the right to freedom of movement, etc.

With regard to the measures envisaged, as set out in Section 7, "Risk Mitigation Measures", we point out that these are not described in sufficient detail, i.e. they are merely listed, without further explanation of what those measures entail and how they will be implemented. From the information provided, it is not possible to determine whether the envisaged measures are adequate in relation to the consequences that could arise if a particular risk materialises, given that, as already noted, neither the possible sources of risk nor the potential consequences have been identified.

In this regard, we point out that it is necessary to reassess and determine appropriate measures, and subsequently to reassess the level of risk, i.e. to evaluate what the level of risk would be after the application of the measures (the so-called residual risk), namely whether it would indeed be "reduced to an acceptable level", as stated in Section 8, "Conclusion of the Assessment".

Accordingly, in the Risk Assessment Act the controller has not provided a comprehensive description of the envisaged processing operations, the purpose of the processing has not been precisely defined, and the assessment of the necessity and proportionality of the processing operations in relation to the purpose of the processing has not been carried out in an adequate manner. Furthermore, the controller has not identified the sources of the identified risks, has not defined the potential consequences for the rights and freedoms of the data subjects, nor the likelihood and severity of their occurrence, and, on that basis, has not determined appropriate measures for their elimination or mitigation. In addition, the opinion of the data protection officer, where such a person has been appointed within the meaning of the Law, has not been provided, inter alia.

All of the above leads to the conclusion that the submitted Data Protection Impact Assessment has not been fully prepared in accordance with the Law on the Protection of Personal Data and that, in the specific case, the conditions for commencing the envisaged processing have not been met.

On this occasion, we also draw your attention to the fact that further information on matters relating to the preparation of a data protection impact assessment may be obtained on the Commissioner's website at www.poverenik.rs, under the "Data Protection" menu – "Guidelines for the Preparation of a Data Protection Impact Assessment".

Case Number: 073-15-2295/2025-02

3.25. Possibility of Using Drones for "Business Purposes"

Question: A commercial company approached the Commissioner seeking an opinion regarding the planned use of a drone "for business purposes", stating, inter alia, that "management is considering the procurement of a drone to be used for: recording the production process, monitoring the condition of warehouses, overseeing facility security, and creating 3D recordings". It was further stated that the recording of "employees' faces" is not envisaged, nor is there any intention to use any recordings for purposes that could infringe employees' privacy, and that access to the recordings would be granted "exclusively to authorised employees". In this context, guidance was requested on the following issues: whether a specific data protection impact assessment (DPIA) is required for this type of recording; which steps must be taken prior to commencing recording; whether employees must be informed and, if so, in what form; and whether any additional notification to the Commissioner is required.

Any data which, directly or indirectly, whether alone or in combination with other information, makes the identity of a natural person determined or identifiable constitutes personal data within the meaning of the cited provision of the Law, and the processing of such data is subject to the principles and rules on processing prescribed by the Law, which must also be borne in mind in the present case. Namely, in the situation described in your submission, even if it were ensured that employees' faces would not be recorded, there remains the possibility that, through the envisaged activities, data could be processed which would render certain natural persons, for example employees, identified or identifiable, that is, that the processing of personal data would take place.

In this regard, we inform you as follows.

First, we point out that the regulations falling within the competence of the Commissioner do not contain specific provisions on video surveillance, nor provisions governing the use of unmanned aerial systems, so-called "drones".

The Law on Private Security, which, inter alia, regulates the performance of activities relating to the protection of persons and property in cases where such activities are not within the exclusive competence of state authorities, provides, as one of the possible methods of technical protection, for "video surveillance" under Article 30, paragraph 1, and further prescribes the manner in which such surveillance may be carried out. Since responsibility for the implementation of the Law on Private Security lies with the Ministry of the Interior, you may contact that authority in order to obtain an opinion on the application of the provisions of the said law.

Furthermore, matters relating to the operation of unmanned aircraft systems, as well as to the liability and registration of the unmanned aircraft system operator, the remote pilot, and similar issues, are regulated by specific legislation, such as the Law on Air Traffic and other relevant regulations. Since inspection supervision over the implementation of that law, the by-laws adopted on the basis thereof, international instruments, and accepted domestic and international standards and recommended practices is carried out by the Civil Aviation Directorate of the Republic of Serbia, through an aviation inspector, you may contact that authority with regard to issues falling within this subject matter.

The Law on Personal Data Protection ("Official Gazette of the RS", No. 87/18), the implementation of which falls within the competence of the Commissioner, regulates, in a systematic manner, the right to the protection of natural persons in relation to the processing of personal data, the principles of personal data processing, and other rules and obligations applicable to controllers and other participants in the processing of personal data, while the processing of personal data in specific fields/activities is regulated by special legislation, the application of which is overseen by other authorities.

From the perspective of the application of the Law on Personal Data Protection, we point out that personal data, within the meaning of Article 4, item 1) of the Law, means any information relating to a natural person whose identity is determined or determinable, directly or indirectly, in particular by reference to an identifier such as a name or an identification number, location data, an identifier in electronic communications networks, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

In this regard, we also point out that, as concerns the processing of employees' personal data carried out by an employer for the purpose of exercising rights and fulfilling obligations arising from employment, Article 91 of the Law on Personal Data Protection provides that, in the field of labour and employment, the provisions of the laws governing labour and employment, as well as collective agreements, shall apply, alongside the application of the provisions of this Law. As the Commissioner is not competent to issue opinions on the application of regulations in the field of labour, you may contact the Ministry of Labour, Employment, Veteran and Social Affairs in order to obtain an opinion on the application of those regulations.

Accordingly, where the processing of employees' personal data is concerned, the employer's authority, in its capacity as controller, for the processing in question should primarily derive from the relevant regulations governing labour, employment and related matters.

From the perspective of personal data protection, we note that, in order for the processing of personal data to be lawful, it is first necessary to ensure that such processing is in compliance with the special regulations governing the relevant field/activity, that the purpose of the processing is specifically defined, explicit, legitimate and lawful, that there is an appropriate legal basis for the intended processing within the meaning of Article 12 of the Law on Personal Data Protection, and that the processing is carried out in accordance with the processing principles laid down in Article 5 of the Law (including the principle of lawfulness, fairness and transparency), as well as with other relevant rules and obligations prescribed by this Law, depending on the circumstances of each individual case.

When it comes to the processing of personal data by means of video surveillance, we note that, generally speaking, the use of video surveillance systems may significantly interfere with the privacy and other rights and freedoms of individuals whose personal data are processed in this manner (e.g. freedom of movement, etc.), in particular where employees' personal data are concerned, bearing in mind that employees have a right to privacy in their working environment. Accordingly, in each individual case it is necessary to assess the necessity and proportionality of such data processing.

Privacy and other rights and freedoms of natural persons may be particularly jeopardised where recording is carried out through the use of unmanned aerial systems, having regard to the area that may be covered by such recording, the mobility of such aircraft as their inherent characteristic, the fact that they may be of very small dimensions and therefore difficult to detect, as well as the camera resolution, zoom capabilities, and the possibility of being equipped with technologies enabling, for example, audio recording, processing of biometric data, reading of IP addresses, RFID technology, artificial intelligence, and similar technologies, all of which may render unmanned aerial systems highly intrusive to the privacy of natural persons.

Accordingly, for each intended processing of personal data, the controller is required, first of all, to determine the purpose of such processing and to assess whether there is an appropriate legal basis for that processing within the meaning of Article 12 of the Law on Personal Data Protection (which has not been specified in your submission), taking into account the special regulations governing the relevant field/activity (including regulations in the field of labour and employment, among others). The controller must also determine whether the processing is necessary for achieving the intended objective, that is, whether the objective for which the introduction of a particular technology is being considered could be achieved in another manner that is less intrusive to the privacy and other fundamental rights and freedoms of the persons whose personal data would be processed by that technology (e.g. the necessity of introducing video surveillance at all, and in particular through the use of unmanned aircraft systems).

We emphasise that your submission does not set out any specific reasons that would justify the use of such a highly intrusive surveillance system, and therefore it cannot be concluded whether the intended processing would in fact be necessary, i.e. indispensable for achieving the purpose of the processing.

Furthermore, with regard to your question concerning the obligation to carry out a data protection impact assessment, we first note that it is unclear what you mean by a "special data protection impact assessment". We also emphasise that the fulfilment of this obligation, which applies in all cases of so-called high-risk processing within the meaning of Article 54 of the Law, would not in itself be sufficient to ensure compliance of the processing with the Law, as the controller must ensure that all of the above-mentioned conditions for the lawfulness of the intended processing are met.

We note that, pursuant to Article 57(1) of the Law, the controller is required to involve the data protection officer in a timely and appropriate manner in all matters relating to the protection of personal data. Furthermore, the data protection officer designated by the controller is, inter alia, obliged

to inform and advise the controller or the processor, as well as employees carrying out processing operations, of their statutory obligations relating to the protection of personal data, in accordance with Article 58(1)(1) of the Law.

Pursuant to Article 5(2) of the Law on Personal Data Protection, responsibility for compliance lies with the controller, who must be able to demonstrate, i.e. prove, that the specific processing is in compliance with the Law. The Commissioner, as the supervisory authority, may adopt a position on a specific processing operation only within the framework of an appropriate procedure falling within his competence (such as an inspection procedure, a complaint procedure, etc.), and on the basis of all facts and circumstances established in that procedure.

Case Number: 073-14-2371/2025-02

3.26. Determining the Status of Controller/Processor in the Provision of Electronic Identification Services

Question: In its request for an opinion, the applicant states that a legal entity, within the scope of its business activities, provides electronic identification services and that among its clients are several operators of special games of chance conducted via electronic communication means. It is further stated that the new rules prescribed by the Law on Games of Chance oblige operators of games of chance conducted via electronic communication means, for the purpose of preventing minors from participating in games of chance, to carry out age verification of users. The applicant further explains that, in order for the legal entity to continue providing adequate electronic identification services to its clients from the online betting industry, it is required to register in the Register of Electronic Identification Service Providers and Electronic Identification Schemes. Such registration is carried out in accordance with the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Business, the Regulation on the Detailed Conditions to Be Met by Electronic Identification Schemes for Certain Levels of Assurance, and the Rulebook on the Register of Electronic Identification Service Providers and Electronic Identification Schemes. It is also stated that the service provider is required to adopt a privacy policy and to regulate in detail, through that policy, all issues relating to the processing of personal data. An opinion was requested in relation to a situation in which a legal entity provides electronic identification services exclusively for the needs of its clients, i.e. performs electronic identification of the end users of its clients (and not its own end users), which gives rise to uncertainty as to whether the provider of electronic identification services would have the role of a controller or a processor.

The status of a party participating in a specific personal data processing operation will depend primarily on the particular tasks for which that party is engaged. Accordingly, where, for example, a party is engaged to perform activities (which involve the processing of personal data) that it carries out pursuant to powers and obligations laid down by specific laws, and where it determines the purpose and/or the means of processing, or where the purpose and/or the means of processing are determined by such specific laws, or where it acts fully independently and autonomously in the provision of its services (without detailed instructions from the entity that engaged it), that party would be considered a controller.

On the other hand, where a party is engaged to perform activities for which no specific obligations or powers are prescribed by special legislation, and where it receives detailed instructions regarding the processing entrusted to it, including the types of personal data to be processed, the categories of data subjects, the duration of the processing, and similar elements, that party would act in the capacity of a processor in respect of such processing.

In this regard, we first inform you that the Law on the Protection of Personal Data (Official Gazette of the Republic of Serbia, No. 87/2018), the implementation of which falls within the remit of the Commissioner, regulates, in a systematic manner, the principles and other general rules of processing, while the processing of personal data in specific fields/sectors is governed by special regulations.

From the perspective of personal data protection, we point out that the concept of a controller is defined by Article 4(1)(8) of the Law on the Protection of Personal Data, pursuant to which a controller is a natural or legal person, or a public authority, which alone or jointly with others determines the purposes and means of the processing. A law which determines the purposes and means of processing may also designate the controller or prescribe the conditions for its designation.

A processor is a natural or legal person, or a public authority, which processes personal data on behalf of the controller (Article 4(1)(9) of the Law). Accordingly, a processor does not determine either the purpose or the means of processing; rather, it is the controller that exercises overall control over the processing, i.e. has a decisive influence over the processing itself.

Where two or more controllers jointly determine the purposes and means of processing, they are considered joint controllers (Article 43(1) of the Law).

When determining the status of participants in the processing, i.e. whether an entity acts as a controller, a processor, or otherwise, it is first necessary to take into account the special regulations applicable in the relevant field. In the present case, in addition to the regulations governing games of chance, it is also necessary to consider regulations in the field of

electronic business (such as the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Business, among others). Furthermore, due regard must be given to the specific type of personal data processing activity carried out in the concrete case, the categories of data subjects whose data are processed, and similar relevant factors.

The determination of the status of participants in a specific personal data processing operation must be assessed by the participants themselves on a case-by-case basis. The Commissioner may adopt a position on this issue only within the framework of a specific procedure falling within his statutory remit, namely an inspection procedure, a procedure conducted following a complaint lodged by a data subject, or another appropriate procedure which he is authorised to conduct in accordance with the Law, and solely on the basis of all facts established in the course of such procedure.

Case Number: 073-14-2465/2025-02.

3.27. Entry/Exit System (EES) – New European Regulatory Framework

Question: The applicant requested an opinion "in connection with the new EU entry rules", stating: "if fingerprints constitute personal data and I do not wish my personal data to be transferred abroad, is there a way to enter the EU without providing fingerprints at the border?", further asking "whether an employer may compel me to waive that right in connection with being sent on a business trip to the EU", and "how I can protect myself from a potential sanction by my employer if I refuse to go on a business trip due to the obligation to provide fingerprints."

In relation to your question "whether there is a way to enter the EU without providing fingerprints at the border", we point out that the protection of personal data within the territory of the European Union is regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (the General Data Protection Regulation – GDPR), as well as by other EU-level regulations and the national legislation of EU Member States. Furthermore, the Entry/Exit System (EES) is regulated by Regulation (EU) 2025/1534 of the European Parliament and of the Council of 18 July 2025 on temporary derogations from certain provisions of Regulations (EU) 2017/2226 and (EU) 2016/399 with regard to the gradual start of operations of the Entry/Exit System.

The aforementioned European Union regulations do not fall within the competence of the Commissioner, nor, pursuant to Article 3 of the Law on Personal Data Protection, does the situation in question concern data processing subject to the application of that Law. Accordingly, this authority has no powers in relation to the application of the said European Union regulations.

In this regard, we first point out that the competences, duties, as well as the inspection and other powers of the Commissioner are laid down in Articles 77–79 of the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia", No. 87/2018). The Commissioner exercises his powers, in accordance with this Law, within the territory of the Republic of Serbia (Article 77, paragraph 1 of the Law).

Article 3 of the Law on Personal Data Protection provides that the Law applies to the processing of personal data carried out by a controller or processor who has its registered seat, or residence or habitual residence, within the territory of the Republic of Serbia, in the context of activities carried out within the territory of the Republic of Serbia, regardless of whether the processing itself takes place within the territory of the Republic of Serbia (paragraph 3). Paragraph 4 of the same Article further provides that the Law also applies to the processing of personal data of data subjects who have their residence or habitual residence within the territory of the Republic of Serbia by a controller or processor who does not have a registered seat, residence or habitual residence within the territory of the Republic of Serbia, where the processing activities relate to: 1) the offering of goods or services to the data subject within the territory of the Republic of Serbia, irrespective of whether payment is required for such goods or services; and/or 2) the monitoring of the data subject's activities, where those activities take place within the territory of the Republic of Serbia.

Therefore, a controller/processor that does not have its registered seat in the Republic of Serbia is subject to the application of the aforementioned Law only if the processing activities relating to the personal data of data subjects who have their residence or habitual residence within the territory of the Republic of Serbia are connected with the offering of goods or services to such persons within the territory of the Republic of Serbia and/or the monitoring of the activities of data subjects, where those activities take place within the territory of the Republic of Serbia.

Having regard to the cited statutory provisions, only where, in a specific case, the processing of personal data falls within the scope of application of the Law on Personal Data Protection of the Republic of Serbia does such processing become subject to the rules governing personal data processing and entail the obligations of controllers and processors of personal data in

accordance with the provisions of that Law, as well as the jurisdiction of this authority.

Further information about the Entry/Exit System (EES), as well as answers to frequently asked questions, can be found on its official website: https://travel-europe.europa.eu/ees

Additionally, with regard to your questions "whether an employer may compel me to waive the aforementioned right due to being sent on a business trip to the EU" and "how I can protect myself against a potential sanction by the employer if I refuse to go on a business trip because of the obligation to provide fingerprints", we point out that matters relating to rights and obligations arising from employment relationships, as well as the processing of employees' personal data by the employer for the purpose of exercising rights and fulfilling obligations arising from employment, are not governed by the Law on Personal Data Protection. Rather, Article 91 of that Law provides that the processing of personal data in the field of employment and labour relations is governed by the laws regulating labour and employment and by collective agreements, with the application of the provisions of this Law.

Supervision over the application of the Labour Law and other regulations on employment relationships, general acts, employment contracts and similar instruments governing the rights, obligations and responsibilities of employees is carried out by the labour inspection. Accordingly, in order to obtain an opinion on the application of those regulations, you may contact the Ministry of Labour, Employment, Veteran and Social Affairs, that is, the Labour Inspectorate.

More detailed information on the competences of the Commissioner and the manner of exercising rights within the Commissioner's remit is available on the official website: www.poverenik.rs.

Case Number: 073-14-2800/2025-02

4. MISDEMEANOUR PROCEEDINGS

The Misdemeanour Proceedings Department is authorised to issue misdemeanour penalty notices and to submit requests for the initiation of misdemeanour proceedings in respect of offences in both areas of human rights protected by the Commissioner. The establishment of this department is the result of legislative amendments granting the Commissioner statutory authority to submit requests for the initiation of misdemeanour proceedings to the competent misdemeanour courts and to issue misdemeanour penalty notices for offences for which the laws within the Commissioner's remit prescribe a fixed monetary fine as a sanction.

4.1. Unlawful processing of personal data – contrary to the processing principle under Article 5(1)(1) of the LPDP – the conditions set out in Article 12 of the LPDP were not met

In an extraordinary inspection supervision, the Commissioner, acting through authorised officials, established that the accused legal entity, acting as the Controller – the housing community – and the responsible person within the legal entity, the professional building manager, carried out unlawful processing of the personal data of apartment owners within the housing community. This was done by disclosing, via email to all residents of the housing community, the personal data of residents who were debtors, namely: their first and last names, addresses, amounts charged, payments made and outstanding debts, although the conditions set out in Article 12 of the LPDP were not met.

In the course of the proceedings, the Controller stated that the personal data in question had been disclosed to the building residents at the insistence of the residents and the investor, and that the purpose of the disclosure was to inform debtors of their outstanding debts.

Article 50(12) of the Law on Housing and Building Maintenance (Official Gazette of the Republic of Serbia, Nos. 104/2016 and 9/2020 – as amended) prescribes that the building manager keeps records of the income and expenditure of the housing community; however, in this case there was no legal basis for making such data available to other persons.

In this manner, personal data were unlawfully processed, contrary to the principle of "lawfulness, fairness and transparency" under Article 5(1)(1) of the LPDP. As a result, the legal entity committed a misdemeanour under Article 95(1)(1) of the LPDP, and pursuant to Article 95(5) in conjunction with Article 95(1)(1) of the same Law, the responsible person within the legal entity is also liable for the misdemeanour.

On the basis of the facts thus established, the Commissioner submitted a request to the competent court to initiate misdemeanour proceedings against the legal entity and the responsible person within the legal entity.

Case Number: 074-01-55/2025-10

4.2. The processing of personal data for the purpose of exercising freedom of expression must be lawful and appropriate, relevant and limited to what is necessary for achieving that purpose of processing.

In an extraordinary inspection oversight, the Commissioner, acting through authorised officials, established that the accused commercial company, which has the status of a legal entity, acting as a personal data controller, together with the responsible person within that legal entity, in the course of its business activities and in the production and broadcasting of content on a YouTube channel, violated the provisions of the LPDP. This was done by failing to process the personal data of a minor in accordance with the principle of "lawfulness, fairness and transparency" referred to in Article 5(1)(1) of the LPDP, and by failing to process the personal data of A.A. and B.B. in accordance with the principle of "data minimisation" referred to in Article 5(1)(3) of the LPDP. By doing so, the accused legal entity committed a misdemeanour under Article 95(1)(1) of the LPDP, for which, pursuant to Article 95(5) of the same Law, the second accused, namely the director and responsible person within the legal entity, is also misdemeanour liable.

During the inspection oversight carried out with regard to the application of the LPDP, it was established that the accused legal entity processed the personal data of a minor, in the form of video recordings of the child's image, as well as data relating to the pre-school institution attended by the child, which were contained in its programmes, in a manner not compliant with the principle of "lawfulness, fairness and transparency". This is because there was no legal basis for processing such data, the minor's legal representatives, i.e. parents, had not given consent for the processing in question, and the personal data concerned did not contribute to the exercise of freedom of expression and the informing of the public. An additional aggravating circumstance is the fact that the data subject is a minor, i.e. a child.

It was also established that the accused legal entity, notwithstanding the fact that it processes personal data in the course of carrying out activities for the purpose of informing the public, did not process the personal data relating to A.A. and B.B. in accordance with the principle of "data minimisation". Specifically, this concerns the processing of data relating to their house number and a video recording of their family home, as well as data relating to the vehicle registration plates of the cars they use, which were included in the programmes produced by the entity. The processing of such data was not appropriate, relevant or limited to what is necessary for achieving the purpose of the processing, namely the exercise of freedom of expression, and in this case the rights and freedoms of the data subjects prevail.

Article 95(1)(1) of the LPDP provides that a controller or processor which has the status of a legal entity shall be fined between RSD 50,000 and RSD 2,000,000 for a misdemeanour if it "processes personal data contrary to the processing principles set out in Article 5(1) of this Law". Paragraph 5 of the same Article provides that the responsible person within that legal entity shall also be fined, for the same misdemeanour, in an amount ranging from RSD 5,000 to RSD 150,000.

Accordingly, the Commissioner submitted a request to the competent court for the initiation of misdemeanour proceedings against both the legal entity and the responsible person within the legal entity.

Case Number: 074-01-1/2025-10

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

342.738(497.11)
342.72/.73.07(497.11)
ЗАШТИТА података о личности : ставови, мишљења и пракса Повереника. Публикација бр. 11 / [уредница Сања Унковић]. - Београд : Повереник за информације од јавног значаја и заштиту података о личности, 2026 (Београд : Службени гласник). - 216 стр. ; 23 cm

Тираж 700. - Стр. 11-12: Уводна реч / Сања Унковић.

ISBN 978-86-82712-07-7

1. Унковић, Сања, 1975- [urednik] [autor dodatnog teksta]
a) Повереник за информације од јавног значаја и заштиту података о личности (Београд) -- Пракса b) Право на заштиту података о личности -- Србија

COBISS.SR-ID 184916233