Pursuant to 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; hereinafter: The "GDPR") and the national legislation of the Republic of Slovenia in the field of personal data protection, in particular the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 163/2022, hereinafter: "ZVOP-2") and in accordance with Articles 12 and 14 of the Decision on the Transformation of the public institute Academic and Research Network of Slovenia into a public infrastructure institute (Official Gazette of the Republic of Slovenia, Nos. 7/23, 124/23, 22/25, 62/25), the Board of Governors of the Academic and Research Network of Slovenia, at its 156th session held on 20 January 2026, adopted the following

RULES

on the Protection of Personal Data

I. General provisions

Article 1

(Scope of the Rules)

(1) These Rules apply to all processing of personal data on behalf of the Academic and Research Network of Slovenia (hereinafter: The "Organisation"), regardless of whether the processing takes place in the European Union or in third countries.

(2) These Rules set out the organisational, technical and logical procedures and measures for the protection of personal data within the Organisation in order to prevent the accidental or intentional unauthorised destruction, alteration or loss of data, as well as the unauthorised access to, processing, use or disclosure of personal data.

(3) Employees who, in the course of their work, process and use the personal and/or confidential data of the Organisation and/or are in possession of trade secrets of the Organisation, are obliged to comply with the provisions of the ZVOP-2, the GDPR, the sectoral legislation applicable to their particular area of work and relating to the protection of personal data, and these Rules and instructions issued on the basis thereof.

Article 2

(Terms and Definitions)

(1) The terms and definitions used in these Rules shall have the following meanings:

a. **Personal data:** Any information relating to an identified or identifiable natural or legal person ("data subject");
b. **Written request or application**: A request or application that is made in writing, in physical or electronic form, and signed by a natural person or by the responsible person of a legal person, with a handwritten or electronic signature;
c. **Controller**: A natural or legal person, public authority, agency or other body that, alone or jointly with
others, determines the purposes and means of processing;
d. **Joint controllers**: Two or more controllers who jointly determine the purposes and means of processing;
e. **Processor**: A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller;
f. **Data Protection Officer ("DPO")**: An appointed person or group of persons who advises the controller in an independent manner to ensure compliance with the GDPR and data protection legislation;
g. **Employee**: Any natural person who has an employment relationship based on an employment contract. For the purposes of these Rules, an employee includes a person who performs work directly for the Organisation on any other legal basis;

h. **External contractors of the Organisation**: Legal and natural persons with whom the Organisation has an agreement to carry out all tasks or a specific task relating to the processing of personal data, in particular to carry out specific processing activities (e.g. contractual processor);

i. **Personal data security incident**: Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

(2) Other terms used in these Rules and defined in the GDPR shall have the same meaning as defined in the GDPR.

II. Responsibilities of the Organisation

Article 3

(Personal data processing conditions)

(1) Personal data may be processed within the Organisation under the conditions laid down in the acts referred to in paragraph three of Article 1
of these Rules.

(2) The processing of data relating to trade union membership is permitted if the data subject has given his/her express written consent (for example, for the purpose of the direct deduction of membership fees from his/her salary) or if this is necessary for the exercise of the obligations and special rights of the controller in the field of employment, and in other cases provided for in the GDPR.

(3) Before entering personal data into the personal data filing system, employees may verify the accuracy of the personal data by consulting the data subject's ID.

(4) Copying personal documents and keeping copies of personal documents is not permitted, except in cases expressly provided for by law. Sending copies of personal documents by email is prohibited.

Article 4

(Obligation to keep records of processing activities)

(1) The Organisation shall keep records of the processing activities in accordance with the provisions of Article 30 of the GDPR. In addition to the information referred to in Article 30 of the GDPR, the record of activities shall contain information on which person is responsible for the processing of personal data and which persons, by virtue of the nature of their work, may process personal data in relation to a particular personal data filing system.

(2) The Organisation has appointed responsible persons (processing administrators) to establish, maintain and update the records of processing activities and the personal data filing systems described in the records of processing activities.

(3) The employees referred to in the previous paragraph shall ensure that the records are periodically reviewed to ensure that they are up to date and that they are entered in the register of records.

(4) The management of the Organisation shall be informed of the updated records at least once a year.

(5) A common register of the Organisation's records of processing activities shall be provided by the Legal Department. The DPO shall be able to
access the common register of records of processing activities.

Article 5

(Obligation to involve the DPO and carry out an impact assessment)

(1) Each department of the Organisation shall be obliged to inform the Organisation's management and the Legal Department before initiating or planning any project in which personal data is or may be processed, and in particular for projects using new technologies or introducing new processing of personal data, which shall seek the opinion of the DPO on the need to carry out a personal data protection impact assessment before implementing the project. In exceptional cases, a department may consult the DPO directly on the need for an impact assessment.

(2) In particular, the DPO shall give its opinion on:

a. Whether an impact assessment is required under Article 35 of the GDPR or Article 87 of the ZVOP-2;
b. The methodology to be used for the impact assessment;
c. Whether the impact assessment should be carried out in-house or with external expertise;
d. What measures (including technical and organisational) should be implemented to mitigate risks
affecting the protection of personal data;
e. Whether the impact assessment has been carried out correctly; and
f. Whether the results or decisions of the impact assessment (e.g., whether to proceed with the processing of personal data / the project on which the impact assessment was carried out) are in line with the GDPR.

(3) The responsibility for (correctly) carrying out the impact assessment lies with the controller.

(4) If the controller disagrees with the DPO's opinion, the controller shall provide written reasons why it does not or will not take the
DPO's opinion into account.

Article 6

(Exercising the rights of data subjects)

(1) The Organisation is obliged to exercise the rights of the data subjects in accordance with Chapter III of the GDPR and in accordance with the ZVOP-2.

(2) Data subjects shall have the right to obtain confirmation from the Organisation as to whether personal data relating to them is being processed and, if so, the Organisation shall provide the data subject with access to the personal data and the information referred to in Article 15(1) of the GDPR and, to the extent consistent with the GDPR, shall grant the following rights:

a. The right to rectification;
b. The right to erasure ("right to be forgotten");
c. The right to restrict processing;
d. The obligation to provide information regarding the rectification or erasure of personal data or the restriction of processing;
e. The right to data portability;
f. The right to object to processing and to automated individual decision-making.

(3) Data subjects shall submit their written request in electronic or physical form in accordance with Articles 15-21 of the GDPR to the Organisation at the address Tehnološki park 18, SI-1000 Ljubljana, with the indication "for the Data Protection Officer" or to the following email address: dpo@arnes.si.

(4) Access to one's own personal data and the exercise of one's rights shall be free of charge for the data subject, but the Organisation may charge a reasonable fee if the request is manifestly unfounded or excessive, in particular if it is repetitive.

(5) If the request does not identify the data subject, the Organisation shall request additional information from the data subject that clearly confirms the identity of the data subject.

(6) After verifying the validity of the request, the Organisation shall provide the data subject with a response no later than one month after the receipt of the request. This deadline may be extended by up to one additional month if necessary, taking into account the complexity and number of requests. The Organisation shall inform the data subject of the extension and the reasons for the delay. The Organisation's decision shall include the reasons and information on the right to lodge a complaint with the Information Commissioner within 15 days of the notification of the decision. The Organisation shall liaise with the DPO, as appropriate, to advise on the preparation of the response. If the Organisation disagrees with the DPO's opinion, it shall provide written reasons for not following the DPO's opinion.

(7) The Organisation may refuse a data subject's request to exercise his or her rights under Chapter III of the GDPR if:

a. The individual cannot be identified as the data subject;
b. The basic conditions are not met (e.g., if the information does not qualify as personal data);
c. The request is manifestly unfounded or excessive; or
d. Specific exceptions are provided for in the GDPR, the Constitution, international instruments or sectoral legislation.

(8) If a data subject believes that their rights have been violated, they can contact the Information

Commissioner for protection or assistance.

Article 7

(Event recording)

(1) For the purposes of documenting activities and publicising the work and events of the Organisation, such as events, meetings, competitions, training, etc., the Organisation may film or photograph such events in whole or in part and publish the resulting material on the Organisation's websites, printed materials and social media.

(2) The fact that the event will be filmed or photographed shall be stated in the invitation or notice of the event. The purpose of the filming or photography shall also be stated. In this way, participants or visitors shall be deemed to have been informed that the public event is being filmed or photographed.

(3) If it is more appropriate (events with a smaller number of participants or events that are not open to the public and where participants have a reasonable expectation of greater privacy), the filming or photographing shall be announced orally and participants shall be given the opportunity to express their wish to be filmed or photographed.

III. Data Protection Officer

Article 8

(Appointment and role of the DPO)

(1) The responsible person of the Organisation shall appoint a Data Protection Officer (DPO) by decision or by other appropriate means (e.g. contract) in accordance with the GDPR and the Personal Data Protection Act and ensure that information about the DPO is published on the Organisation's website.

(2) The DPO shall assist in the implementation of key elements of the GDPR, such as:

a. Principles governing the processing of personal data;
b. Data subjects' rights;
c. Security and records of personal data processing;
d. Notification of personal data breaches.

(3) The Organisation shall ensure that the DPO is adequately and timely involved in all matters relating to the protection of personal data, is provided with the appropriate resources necessary for the quality performance of his/her duties and is granted access to personal data and processing operations.

(4) The DPO shall not be responsible for ensuring that the processing of personal data complies with the rules of the GDPR and the applicable Act governing the processing and protection of personal data. The responsibility for ensuring such compliance rests with the Organisation or the responsible person of the Organisation under applicable law.

Article 9

(Tasks of the DPO)

(1) In particular, the DPO shall:

a. Inform the Organisation of its obligations to implement the provisions of the GDPR and other applicable data protection legislation, as well as the internal acts governing the processing and protection of personal data;
b. Oversee the compliance of the protection of personal data with the applicable laws and internal acts, including assigning tasks, advising employees on the correct processing of personal data and monitoring the protection of personal data in the Organisation;
c. Advise on and monitor the implementation of the data protection impact assessment;
d. Act as a point of contact for the Information Commissioner and in particular liaise with the Information Commissioner on issues relating to the processing of personal data, prior consultation on impact assessments where a particular processing of personal data would present a high risk, or on any other matter relating to the protection of personal data;
e. Inform the Information Commissioner about any breaches of the processing of personal data and cooperate with the Information Commissioner in remedying such breaches.

(2) The DPO shall perform the duties set out in the previous paragraph of this Article in relation to all processing of personal data carried out by the Organisation.

(3) In the performance of his/her duties, the DPO shall be obliged to protect as a trade secret all information of which he/she becomes aware in the performance of his/her duties.

Article 10

(Independence of the DPO)

The Organisation shall ensure that the DPO receives no instructions in the performance of his/her duties. The DPO shall not be dismissed or sanctioned for the performance of his/her duties. The DPO shall report directly to the responsible person of the Organisation.

IV. Services provided to the Organisation by other legal or natural persons

Article 11

(Processors)

(1) A written contract or other legal instrument containing or supplementing the information provided for in paragraph three of Article 28 of the GDPR shall be concluded with any legal or natural person outside the Organisation who carries out specific tasks relating to the collection, processing, storage or transmission of personal data on the instructions of the Organisation (processors).

(2) The provisions of the previous paragraph shall also apply to external persons who maintain hardware and software and who develop and install new hardware or software, provided that they have access to personal data.

(3) External legal or natural persons may only provide personal data processing services within the scope of the authorisation of the Organisation and the specified scope of the category of personal data and may not process or otherwise use the personal data for any other purpose. External legal or natural persons may not delegate to another processor without the prior written consent of the Organisation, unless the possibility of delegation to another processor is already provided for in the contract between the controller and the original processor.

(4) A legal or natural person providing agreed services to the Organisation outside the premises of the controller shall
have at least the same level of protection of personal data as provided for in these Rules.

Article 12

(Joint controllers)

(1) When the purposes and means of processing are jointly determined by the Organisation and other legal entities for an individual processing operation, the Organisation and the other legal entities are joint controllers for that processing operation for the purposes of these Rules.

(2) In order to fulfil their obligations and in accordance with the rules of Article 26 of the GDPR, the joint controllers shall determine in a transparent manner and by mutual agreement the duties of each of the joint controllers.

Article 13

(Contract monitoring)

All contracts relating to the contractual processing of personal data and the joint management of personal data entered into by the Organisation shall be recorded in a contract register managed by the Legal Department. The DPO shall have access to the contract register.

V. Responsibility for the implementation of security measures and procedures

Article 14

(Obligations of the Organisation)

(1) The Organisation shall regularly inform and train its employees on the importance of and new developments in the area of personal data protection.

Article 15

(Appointment of processing administrators)

(1) In order to implement the procedures and measures for the protection of personal data, the responsible person of the Organisation shall designate the persons responsible for each processing of personal data, who shall be informed of and shall be accountable for the content, purpose and grounds of each processing operation (processing administrators – as listed in the record of processing activities).

Article 16

(Obligation of all employees)

(1) Every employee who processes personal data on behalf of the Organisation shall be obliged to implement the prescribed procedures and measures to safeguard the data and to protect the data of which he/she has knowledge or of which he/she becomes aware of in the course of his/her work. Such an employee shall treat the personal data of which he/she becomes aware in the course of his/her work with diligence and care, in the manner and according to the procedures established in these Rules and the related documents.

(2) Before starting work, employees shall sign a special declaration in which they undertake to protect personal data and are warned of the consequences of failing to do so.

(3) Employees may only process personal data that is necessary for the performance of their duties.

(4) The obligation to protect personal data that employees access or become aware of in the course of their work shall continue after their relationship with the Organisation has ended.

Article 17

(Disciplinary liability)

(1) Any failure to comply with the provisions of the internal information security documentation and the instructions and procedures for the protection of information or personal data shall be considered a breach of the employment obligations in accordance with the regulations and general acts governing breaches of contractual and other obligations arising from the employment relationship.

(2) In particular, it shall be considered a serious breach if the employee:

- Discloses personal data he/she has become aware of in the course of his/her work to other persons
  without authorisation;
- Makes unauthorised copies of personal data media;
- Makes unauthorised corrections, alterations or additions to personal data;
- fails to notify the authorised person for information security at Register.si (in the case of a breach in an area covered by the Register.si sector) or the SUVI (Information Security Management Service) administrator (for the remaining part of Arnes) about the misuse of personal data or an intrusion into a personal data filing system.

(3) The liability referred to in the previous paragraphs shall not exclude criminal liability, liability for infringement and/or liability for damages.

Article 18

(Access to the personal data of employees in exceptional cases)

(1) In exceptional cases (sudden termination

of employment by an employee, the death of an employee, the unexpected, sudden and prolonged or permanent absence of an employee, termination of employment by the employee without notice, termination of employment for misconduct due to unexcused absence and similar exceptional cases), employees with management rights/access to the service may, at the specifically justified written request of the responsible person of the Organisation, in the presence of a committee of three members, access the information technology (e.g. computer) or other electronic or communication services (e.g. email) of the employee if this is strictly necessary for the fulfilment of the Organisation's legal obligations or for the management of the work process.

(2) Access shall be carried out by a committee of three members, each appointed by the responsible person in the Organisation. It shall include at least one employee representative who is not a manager. The committee shall keep a record of the access, which shall include the following:

- An explanation of the reason for the access;
- A record of the access with any comments made by the employee, if present;
- Comments of any persons present;
- A list or extract of the data obtained.

(3) If there are reasonable grounds to suspect that an employee is not complying with the provisions of the internal information security documentation, an employee with management rights/access to the service may, at the specific and justified written request of the responsible person of the Organisation, monitor the use of the electronic services, but only with a view to checking the logs of traffic volume and stored data loaded on the server. The content may not be monitored.

(4) The Organisation may only request access to the telephone traffic data of telephone lines owned by the Organisation from the telecommunications service providers or the PBX maintenance company if there is a dispute between the Organisation and the employee as to the amount of charges for the use of a particular telephone line.

VI. Video surveillance

Article 19

(Video surveillance)

(1) Video surveillance may be introduced in the Organisation if the conditions set out in the GDPR and in Chapter 3 of Part II of the ZVOP-2 are met.

(2) Details regarding the operation, management and supervision of the video surveillance system are governed by internal
documentation regulating the field of video surveillance.

VII. Receipt and transmission of personal data

Article 20

(Receipt and recording of physical mail)

(1) The rules for the receipt and recording of postal items and items received by other means (brought by customers or couriers) are set out in an internal document governing the procedures for the receipt and delivery of postal items.

Article 21

(Transmission of personal data)

(1) Personal data may be only transmitted by information, telecommunication and other means if procedures and measures are in place to prevent unauthorised persons from obtaining or destroying the data and from having unauthorised access to its contents.

(2) Personal data shall be transmitted in a manner that does not allow access by unauthorised persons. Personal data transmitted in physical form shall be transmitted in an envelope. The envelope shall be designed in such a way that the contents of the envelope are not visible in daylight or when the envelope is illuminated by

an ordinary light. The envelope shall also ensure that it cannot be opened and its contents examined without leaving a visible trace of the opening of the envelope.

(3) Personal data may be transmitted over telecommunication networks and, in the case of sensitive personal data and/or a large volume of personal data, the personal data shall be protected using cryptographic methods in such a way as to ensure that it is unintelligible during transmission.

Article 22

(Transmission of special categories of personal data)

(1) In addition to the provisions of the previous paragraph, special categories of personal data pursuant to Article 9 of the GDPR or personal data relating to criminal convictions and offences pursuant to Article 10 of the GDPR shall be physically sent to the addressees in sealed envelopes against signature in a delivery book or by registered mail with return receipt requested.

(2) Special categories of personal data may only be transmitted over telecommunication networks if they are specifically protected by cryptographic methods to ensure their unreadability during transmission.

(3) In order to guarantee the integrity of the personal data referred to in the previous paragraph, an electronic signature
shall be used where appropriate and within the technical possibilities of the sender and the recipient.

Article 23

(Disclosure of personal data to third parties)

(1) The Organisation shall disclose personal data to other public sector bodies or to other natural or legal persons (third parties) if there is an adequate legal basis for the disclosure in accordance with the legislation governing the protection of personal data, unless another law provides otherwise. Personal data may also be disclosed to third parties who have the consent (authorisation) of the data subject. The third party may only process the personal data for the purpose for which it was disclosed.

(2) The third party shall request the disclosure of personal data in writing. The request must contain all the elements required by the legislation on the protection of personal data. If the third party has obtained the data subject's consent to the disclosure of personal data, the data subject's consent (authorisation) must be attached to the written request.

(3) Unless otherwise required by another law, the Organisation shall disclose the requested personal data to the third party no later than 15 days after receipt of a complete request or, within that period, shall provide the third party with written notice of the reasons for not disclosing the requested personal data to the third party. The Organisation and the third party may agree to extend this period. If the Organisation fails to provide the information within 15 days, or if the period is not extended, the request shall be deemed to have been denied.

(4) For each disclosure of personal data, it must be possible to establish at a later date what personal data was disclosed, to whom, when and on what basis and for what purpose or for what reasons, or for the purposes of what procedure.

(5) Original documents shall never be disclosed unless ordered to do so in writing by a court of law. Original documents shall be replaced by a copy while they are unavailable.

Article 24

(Transfer of personal data to third countries or international organisations)

(1) The transfer of personal data to third countries or international organisations is permitted under the conditions
set out in Chapter V of the GDPR.

(2) The DPO shall be consulted prior to any proposed processing operation that will or may transfer personal data to a third country or international organisation.

VIII. Security of premises and computer equipment

Article 25

(1) The premises in which personal data media, hardware and software are located (secure premises) shall be protected by organisational and physical and/or technical measures in order to prevent unauthorised persons from gaining access to the data.

(2) The security of premises and computer equipment is defined in more detail in the internal information security documentation.

IX. Protection of system and application software and data processed by computer equipment

Article 26

(1) System and application software, as well as data processed by computer equipment, shall be protected by organisational and physical and/or technical measures that prevent unauthorised persons from accessing the data.

(2) The protection of system and application software and data processed by computer equipment is defined in the internal information security documentation.

X. Measures to be taken in the event of suspected unauthorised access and notification

Article 27

(Measures to be taken in the event of a suspected incident)

(1) Any suspected intrusion into the Organisation's information system or any other security incident involving or likely to involve a personal data breach (the unauthorised processing, disclosure of personal data, etc.) shall be investigated as soon as it becomes known.

(2) Investigations shall be conducted in accordance with:

a. These Rules;
b. Internal information security documentation.

Article 28

(Detection and notification of a breach)

(1) Any employee who becomes aware of or observes that a personal data protection breach has occurred or that there has been an intrusion into a personal data filing system shall immediately notify the authorised person. If the breach concerns an area covered by the Register.si sector, the employee shall notify the authorised person for information security at Register.si; in all other cases, the SUVI (Information Security Management Service) administrator at Arnes shall be notified.

(2) Following an initial triage of the potential personal data protection breach, the authorised person referred to in the preceding paragraph must,
as soon as possible, notify the DPO and inform the Legal Department thereof.

(3) During the handling of a personal data protection breach (incident), the following information shall in particular be collected and communicated in the notification referred to in the previous paragraph: the data necessary to identify the personal data affected by the breach, a brief description of the circumstances in which the breach occurred, whether the employee responsible for maintaining the personal data filing system has been informed of the breach, and which measures to prevent further personal data protection breaches have been implemented.

(4) If a personal data breach has occurred at the processor, the processor shall notify the Organisation in writing within 24 hours of becoming aware of the breach. Such a provision should, where possible, be included in every data processing agreement concluded by the organisation with a processor after the entry into force of these Rules.

(5) The Organisation shall ensure that all measures are taken to prevent further breaches of the protection of personal data and to take appropriate action against anyone who has, intentionally or through gross negligence, breached the protection of personal data. The obligations in this paragraph shall also apply to processors and joint controllers.

(6) The Organisation shall document any personal data breach, including the facts relating to the personal data breach, its impact and the corrective measures taken. The Organisation shall make this documentation available to the DPO or Information Commissioner upon request.

(7) All employees involved in the investigation of an incident, or in any way involved in the remediation of an incident, shall inform the authorised person referred to in paragraph one of this Article in accordance with the internally agreed procedure, and the latter shall, where necessary, inform the DPO.

Article 29

(Notification to the supervisory authority)

(1) In the event of a perceived personal data breach, the Organisation shall, in consultation with the DPO, notify the Information Commissioner of the breach no later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to compromise the rights and freedoms of the data subjects, in accordance with the provisions of Article 33 of the GDPR.

(2) The Organisation shall provide all necessary information for the notification referred to in the previous paragraph and complete the breach notification form, with the assistance of the DPO and other relevant parties.

(3) If the information referred to in paragraph one of this Article cannot be provided in full to the Information Commissioner, it shall be provided in stages.

Article 30

(Notification of an incident under the Information Security Act)

(1) In the event of a breach of personal data relating to the information system referred to in paragraph one of
Article 23 of the ZVOP-2, the provisions of the Information Security Act relating to essential entities shall apply mutatis mutandis with regard to the notification of an incident, if the Organisation is not required to implement measures under the Information Security Act with regard to these processes.

(2) The Organisation shall also be required to comply with the incident notification provisions of the Information Security Act for other personal data breaches for which it is required to implement measures under the Information Security Act with respect to the processing of personal data.

Article 31

(Informing data subjects)

(1) The Organisation, in cooperation with the DPO, shall assess, as part of the incident evaluation, whether the personal data breach is likely to have resulted in a significant risk to the rights and freedoms of data subjects, and thus whether the conditions for notifying the data subjects have been met.

(2) If the conditions for notifying the data subjects referred to in the previous paragraph are met, the Organisation shall notify the data subjects of the personal data breach without undue delay.

(3) The content and method of notifying the data subjects shall be agreed between the Organisation and the DPO, taking into account the provisions of Article 34 of the GDPR.

(4) The Organisation shall record in the documentation referred to in paragraph six of Article 28 of these Rules all the facts
and the reasons for the decision to inform or not to inform the data subjects.

XI. Erasure of data

Article 32

(Respecting retention periods)

(1) Upon the expiry of the retention period or the purpose of the processing, personal data shall be erased, destroyed, blocked or made anonymous, unless otherwise provided by law or another act. The Organisation shall limit the retention period of personal data to the shortest possible period and only for as long as the retention is necessary to achieve the purpose of the processing for which the data was collected or further processed.

(2) The time limits for the erasure of personal data from the filing system shall be indicated in the records of the processing
activities.

(3) If the time limits for the erasure of personal data are expressed in years, the time limit for erasure shall run from the end of the calendar year
in which the case was closed.

Article 33

(Safe and secure media destruction)

(1) The method of erasure or anonymisation used to delete data from information systems shall be such that it is impossible to recover or de-anonymise all or part of the erased data. For the destruction of data storage media, a method shall be used that makes the restoration of the data impossible.

(2) Data on traditional media (documents, files, registers, inventories, etc.) shall be destroyed in such a way as to make it impossible to read all or any part of the destroyed data (incineration, shredding, etc.). Supporting material (e.g. matrices, calculations and graphs, sketches, test or error printouts, etc.) shall be destroyed in the same way. Employees may destroy physical documents containing personal data themselves, provided that they are not documentary or archival material.

(3) It is forbidden to dispose of waste media containing personal data in the rubbish bin.

(4) When transferring media containing personal data to a destruction facility, appropriate security shall also be provided at the time of transfer.

(5) The transfer of the media to the destruction site and the destruction of the personal data media shall be supervised by a person from the department or sector authorised by the Director. After the destruction, this person shall make a brief record of the manner of the destruction.

XII. Final provisions

Article 34

(Validity of the Rules and expiry of the existing Rules)

(1) The specific procedures and measures for the protection of personal data held in the personal data filing system managed by the Organisation, as referred to in these Rules, are set out in the internal information security documentation.

(2) On the date of adoption of these Rules, the existing Rules on the Protection of Personal Data of 6 November 2024 shall cease to apply.

(3) These Rules shall enter into force on the date of their adoption.