Data Protection Rules

Slovenian Society for Stereology and Quantitative Image Analysis, Korytkova ulica 2, 1000 Ljubljana, registration number: 5669910000, (hereinafter: "controller") on the basis of Articles 24 and 25 of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 94/07 with amendments, hereinafter: " ZVOP-1") and in particular Articles 24, 25 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals in the processing of personal data and on the free flow of such data and on the repeal of the Directive 95/46/EC (hereinafter: "General Data Protection Regulation")

accepts the following

Data Protection Rules

I. Regarding the processing of personal data

Article 1

The controller is a society that is engaged in the main activity of "activities of professional associations", whereby the processing of personal data of the controller is only a side process.

The controller primarily performs the following personal data processing actions:

- Processing of personal data entered by the authors themselves via the online form,
- searching and recording personal data of reviewers through publicly available information (personal websites of researchers, contact data published in scientific publications).

The controller does not transfer or export the data to third countries and/or international organizations.

When performing the above-mentioned activities, the manager processes the following personal data:

- Name and surname,
- title,
- electronic address,
- affiliation,
- area of expertise,
- gender.

The operator does not process special types of personal data (so-called sensitive personal data), nor does it process personal data related to criminal convictions and misdemeanors.

The controller processes personal data on the basis of legitimate interest or consent for the following purposes:

- Editorial process (peer review),

- contacting authors and reviewers,
- notification of the publication.

Article 2

For the purpose of identification and inventory of all types of personal data processed by the controller, a List of records of personal data processing activities (hereinafter: "List of records") is kept, the purpose of which is to enable a complete overview of the processing of personal data. The list of records is also the basis for adopting technical, organizational, and personnel measures to secure personal data, as described in this Data Protection Rules (hereinafter: the "Rules").

The controller ensures the List of records is accurate and up-to-date. The controller will grant access to the List of Records to the supervisory authority at its request.

The editorial team who processes personal data in the performance of work and tasks for the controller must be familiar with the List of Records. Access to the List of Records must be made available to anyone who requests it and shows a legitimate interest (e.g. the individual to whom the personal data relates, supervisory authority, or police based on statutory powers).

Article 3

Taking into account the nature, scope, circumstances, and purpose of the processing, the controller concludes that the processing of data does not pose a major risk to the rights and freedoms of individuals, therefore a preliminary impact assessment in relation to the processing is not required.

Before any new processing of personal data, and in particular before the use of new technologies and before any change in the nature, scope, circumstances, and purposes of the processing, and whenever the risk posed by processing actions changes, the controller undertakes to conduct a risk review and assess, whether it is necessary to prepare an impact assessment in relation to the processing.

II. General provisions

Article 4

These Rules determine the technical, organizational, and personnel procedures and measures for the protection of the controller's personal data, with the aim of fulfilling the legal requirements regarding the protection of personal data and protecting the rights of individuals to which refers to personal data.

These measures consist of binding rules, recommendations, or principles from practice, internal procedures, organizational structures, and information technology security.

Article 5

The purpose of these Rules is to ensure the confidentiality, integrity, accessibility, and accuracy of personal data. All editorial team must be aware of the risks associated with technical and information systems and communication technology and must therefore carry out the processing of personal data with the required care.

The measures described in these Rules are designed taking into account the latest technological development and costs, implementation, and the nature, scope, circumstances, and purposes of processing as well as risks to the rights and freedoms of individuals and ensure adequate data security in relation to the potential risks posed by data processing, especially in case of accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data that is sent, stored or otherwise processed.

Article 6

The controller follows the recognized rules for information security.

In addition to practical experience, the manager follows the following standards in ensuring the security of information technology:

- Arnes server secure TLS connection
- Incoming mail server, IMAP server, with secure SSL connection.

Article 7

When processing personal data, the controller observes the general principles regarding the processing of personal data.

The controller processes only personal data for which it has an appropriate legal basis based on the provisions of ZVOP-1 and the General Data Protection Regulation.

Personal data may only be collected for specified and lawful purposes and may not be further processed in such a way that their processing is inconsistent with these purposes unless otherwise provided by relevant legislation.

When processing personal data, the controller ensures that the personal data:
• processed legally, fairly, and in a transparent manner in relation to the individual to whom the personal data refer;
• collected for specific, explicit, and legal purposes and not to be further processed in a way that is incompatible with these purposes;
• adequate, relevant, and limited according to the purposes for which they are processed;
• accurate and, when necessary, updated;
• kept in a form that allows the identification of the individuals to whom the personal data relate, only as long as this is necessary for the purposes for which they are processed unless the individual law provides otherwise;

• processed in a way that ensures their integrity and confidentiality, and in particular, that they are properly protected against unauthorized or illegal processing and against accidental loss, destruction, or damage with appropriate technical or organizational measures.

Article 8

These Rules apply to all members of the Society, editors, reviewers, and authors, regardless of whether they are still active at the operator (hereinafter "collaborators").

Article 9

The terms used in these Regulations have meanings derived from the valid ZVOP-1 and the General Data Protection Regulation.

III. Personnel measures

Article 10

Tasks and powers regarding the processing of personal data, which are in conflict with each other, are assigned to different persons or departments; all with the aim of identifying unauthorized or unintentional data changes as soon as possible.

The following separation of tasks applies:
• the purposes of personal data processing are determined by the controller's editorial board;
• the authority to determine information technology resources or operational processes is assigned to technical editors,
• the president of the Society is responsible for data security and ensuring technical, personnel, and organizational measures,
• the following persons have access to personal data: the president of the association and the editors.

The president of the Society is ultimately competent and responsible for the correct implementation of these Rules.

Article 11

Since the processing of personal data by the controller does not include regular and systematic extensive monitoring of individuals and since the controller does not process special types of personal data and/or data related to criminal convictions and misdemeanors, the controller will not appoint a specially authorized person for data protection.

Article 12

All members of the Society who act under the guidance of the controller and have access to personal data may not process this data without or outside of the controller's instructions.

The obligation to protect data does not end with the termination of cooperation.

All members of Society who process personal data during their work must be familiar with the legislation in the field of personal data protection and the content of these Rules.

In accordance with the principle of responsibility, the controller will, if necessary, provide employees who handle personal data with appropriate training or trainings in the field of personal data protection.

Members of the Society are disciplinary, compensatory, and criminally liable for the violation of the provisions of this article.

IV. Physical and environmental security

Article 13

Personal data and information systems must be adequately protected against theft, damage, and negative effects from the environment.

The premises where personal data, their copies, and information systems are located, must be fireproof (fire extinguishers, fire sensor), protected against water spills, floods, and electromagnetic disturbances, within the prescribed climatic conditions, and locked.

All information systems that are critical for the manager must be placed in a secure environment. This means that all premises in which personal data carriers and hardware and software are located are physically protected (e.g. locked, stored in a safe, etc.), so that unauthorized persons are prevented from accessing the data.

Such protected premises, or the building as a whole, where personal data is stored, are equipped with a device for reporting burglaries and video surveillance or with the physical presence of a security guard. On the basis of such measures, it is possible to trigger an alarm and secure evidence.

Article 14

Personal data must not be stored outside of secure areas.

V. Protection of data integrity and confidentiality upon receipt and transmission

Article 15

Personal data is transferred by means of telecommunications and other means, with the implementation of appropriate procedures and measures that prevent unauthorized persons from misappropriating or destroying the data, as well as unauthorized access to their content.

In the case of sending electronic messages with personal data, the controller provides technical procedures that prevent the interception, copying, modification, redirection, or destruction of the transmitted information. These procedures are, for example:

- Incoming mail server, POP3 server with secure SSL connection,
- outgoing mail server, SMTP server, with secure SSL connection (SMTP over SSL) – with SMTP authentication,
- outgoing mail server, SMTP server, with secure TLS connection (mail submission port) – with SMTP authentication,
- incoming mail server, IMAP server, with secure SSL connection.

VI. Ensuring accessibility or data availability in the event of a physical or technical incident

Article 16

Personal data is provided only to those who prove to have an appropriate legal basis or with a written request or consent of the individual to whom the data relates.

Every transmission of personal data is recorded in the records of transmissions, which must show which personal data were transmitted, where or to whom, when, and on what basis. Records of the traceability of data transfers are kept in chronological order.

Original documents are never provided, except in the case of a written court order. The original document must be replaced by a copy during the absence.

Article 17

For the needs of restoring the computer system in the event of breakdowns and in other exceptional situations, regular copies of the content of the network server and local stations, if the data is located there, are guaranteed (i.e. making backup copies of the data).

For data subject to a high availability requirement, a backup copy must be established regularly, so that in the event of a failure of one or more components, the operational readiness of the entire system can be restored.

Article 18

In the event of a system failure, it must be ensured that no critical information is lost.

Backup storage media must be kept in locations that meet the requirements of confidentiality, integrity, and availability of the information in question. This also includes a sufficient spatial separation between the backup storage media and the backup source (eg storage in other rooms).

Article 19

Data is archived in accordance with legal, contractual, and business requirements.

Archive data must be stored or stored in places that meet the requirements of availability, integrity, and confidentiality.

VII. Regular testing, assessment, and evaluation of measures

Article 20

The controller undertakes to regularly test, assess and evaluate the effectiveness of technical and organizational measures to ensure processing security.

For this purpose, the controller will check the legality of personal data processing at least once a year.

VIII. Retention period and deletion of data

Article 21

The controller ensures that the period of personal data storage is limited to the shortest possible period.

After the expiration of the retention period, personal data are deleted or permanently destroyed, or anonymized, unless the law or other act stipulates otherwise.

Article 22

To delete data from computer media, such a deletion method is used that it is impossible to restore all or part of the deleted data. Deletion must be complete and irreversible. In addition to the holder of such data, it is also necessary to destroy the data in the "Deleted" or "Trash" folder or other relevant folder/directory, so that the content can no longer be restored.

IX. Services provided by external legal or natural persons

Article 23

The controller can also entrust individual data processing actions to an external legal or natural person (hereinafter: "processor"), which provides sufficient guarantees for the implementation of appropriate technical and organizational measures for the protection of personal data. A processor that provides agreed services outside the operator's premises must have at least as strict a method of protecting personal data as provided for in these Rules.

In such a case, the controller will enter into appropriate written agreements with the processor on the contractual processing of personal data, in which they will determine the rights and obligations of both parties. In such an agreement, conditions and measures must be prescribed to ensure the protection of personal data and their insurance, as well as the obligations of the processor towards the controller. The aforementioned also applies to processors who maintain hardware and software and manufacture and install new hardware or software.

On the basis of such an agreement, the processor can only perform the agreed tasks in the name and on behalf of the controller in connection with the processing of the personal data of the controller. The processor may not process or otherwise use the data for any other purpose.

X. Reporting in the event of a security incident

Article 24

The controller shall ensure a consistent and effective system for handling security incidents, including the documentation and notification of security incidents.

For this purpose, the controller shall provide an information system capable of monitoring events (e.g. firewall, intrusion detection, monitoring system). Information systems also enable the documentation of all security-relevant or system-critical events.

The controller records every violation of personal data protection in the security incident record, which must show the facts related to the violation of personal data protection, the effects of such a violation, and the corrective measures taken.

All security incidents are entered in the security incident record in chronological order, regardless of the level and type of risk to the rights and freedoms of individuals. In particular, the controller records violations of data confidentiality (e.g., unauthorized disclosure of data), violations related to the possibility of accessing data, and violations of data integrity (e.g., unauthorized modification of data).

Article 25

If it is likely that the rights and freedoms of individuals would be threatened by a breach of personal data protection, the controller must immediately, and at the latest within 72 hours after becoming aware of the breach, notify the competent supervisory authority about it, in accordance with Article 33 of the General Regulation on Protection data.

When it is likely that a breach of the protection of personal data causes a high risk to the rights and freedoms of individuals, the controller must, in accordance with the provision of Article 34 of the General Data Protection Regulation, also inform the individuals to whom the personal data relate without undue delay that a breach has occurred protection of personal data.

XI. Final Provisions

Article 26

All amendments and additions to these Rules are accepted in the same way as the Rules and in writing.

Article 27

The Rules come into force on the eighth (8th) day after the president of the Society accepts and publishes them.

The rules are published in the controller's usual way, namely on the website https://www.ias-iss.org/ojs/IAS/about/editorialPolicies#custom-5 so that all members of the Society, reviewers, and authors can familiarize themselves with its content.

In Ljubljana, on 20. March 2023

Marko Kreft, president of the Society