THE REGULATIONS

on the security and processing of the personal data at the BIOIRC DOO

Chapter I - GENERAL PROVISIONS

Article 1 (*Scope of the policy*)

The BIOIRC DOO through its research and development activities as well as fundamental, development and applied research work acts as the manager of personal data.

These regulations define organizational, technical and logical-technical procedures and measures for the security of personal data with the aim of prevent accidental or intentional unauthorized processing of personal data, their change or loss, as well as unauthorized access or loss of access.

Employees and external collaborators who process personal data in the course of their work must be familiar with the Regulation, the law governing the protection of personal data, with the regional the legislation governing the individual area of their work and the content of this rulebook.

Article 2 (*Meaning of terms*)

The terms used in this regulation have the same meanings as defined in Article 4 of the Regulation.

"Carriers of personal data" are paper or electronic documents, hard disks, electronic portable memory devices (eg USB, portable data drives), software and other recordable and storage media personal information.

"Workstation" is a computer, laptop, tablet or other similar device that, in addition to recording and storage, enables also other processing of personal data (e.g. display).

A password is a set of characters consisting of letters, numbers and other characters and is based on a secret known to the user.

External contractor (contractual contractor) means an individual or company that is responsible and in charge of assigning and restricting access rights to applications and data of the personal data manager and other information systems.

Chapter II - AUTHORIZED PERSON FOR DATA PROTECTION

Article 3 (*DPO appointment*)

The BIOIRC DOO director appoints the Authorized Person for data protection (hereinafter: DPO).

A person who meets the conditions set out in the Regulation and the Act governing the protection of personal data may be appointed as DPO, and must have experience in the field of personal data protection, and it is also recommended in the field of information systems security.

Article 4 (*Tasks and position of DPO*)

DPO implements for BIOIRC DOO following:

- tasks specified by the Regulation and the law governing the protection of personal data,
- prepares an annual work plan based on the risk assessment and submits it to the director,
- annually reports on his work to the director.
- advises scientific-research and professional-technical staff on issues related to data security,

- monitors the compliance of conduct in the field of personal data protection,
- implements data security related measures,
- organizes employee training and informing employees about the handling of personal data,
- provides information about detected violations of the data security.

DPO may not be dismissed or punished for performing his duties.

DPO must be guaranteed access to personal data and processing actions carried out by the BIOIRC DOO.

Article 5 (*contact details of the DPO*)

The BIOIRC DOO publishes the name, surname and contact information of the DPO on the BIOIRC DOO website.

Chapter III - SECURITY OF PREMISES AND COMPUTER EQUIPMENT

Article 6 (*Premises security*)

Premises where carriers of protected personal data and hardware and software are located (hereinafter referred to as: protected premises) must be protected by organizational, physical and technical measures that prevent unauthorized persons from accessing the data.

Unemployed persons may not enter secured premises without being accompanied or in the presence of an employed worker. An employee who works in protected areas must conscientiously and carefully control the area and lock the area when leaving the area.

Maintainers of premises and other equipment in protected premises, business partners and other visitors may move in secured premises only in the presence of an employee of the institution.

Employed technical-maintenance workers and cleaners may move in secured premises outside of working hours and without the presence of the responsible worker only if the data carriers are stored in locked cabinets and the workstations are locked, in the manner specified in these regulations for the time outside working hours.

Access to the premises referred to in paragraph 1 of this article is possible and permitted only during working hours, and outside of working hours only on the basis of the permission of the BIOIRC DOO director.

Holders of personal data stored outside active work areas or outside protected areas (corridors, common areas, active and passive archives, etc.) must be permanently locked in a fireproof, protected cabinet.

The keys to the secured premises are kept in the premises specified by the house rules of the BIOIRC DOO, unusable keys are destroyed by the committee. Keys are not left in the door lock from the outside.

Secured premises must not remain unattended, or must be locked in the absence of workers who they control.

Article 7 (*Handling data carriers*)

Outside of working hours, personal data carriers must be stored in secure workplaces.

Computers or other hardware on which personal data is processed or stored must be switched off and physically or software locked outside of working hours, and access to personal data stored on workstations must be coded.

Computers that must be connected at all times due to constant access must be protected in the sense of the first paragraph Article 6.

Employees must not leave personal data carriers (including documents) on desks in the presence of persons who do not have the right to view them (e.g. customers). Every time the employee leaves his workplace, he must ensure that there is no personal data on the desk or other work surface ("clean desk" policy), including the carriers of personal data collections, and the workstation (computer) is programmatically locked or turned off (policy “blank screen”).

In the premises to which customers or persons who are not employed by the BIOIRC DOO have access, data carriers and computer displays must be installed during processing or work on them in such a way that customers are prevented from viewing them.

Data carriers containing special types of personal data must be specially marked and secured.

Article 8 (*Processing space*)

Processing of personal data from personal data collections is permitted only on the premises of the BIOIRC DOO.

An exception to the provisions of the first paragraph of this article is permitted if the export of the carrier and/or the processing of personal data outside the institution is expressly permitted in advance by the director of BIOIRC DOO.

When an employee takes data carriers out of secured premises and/or processes personal data outside the premises, he must ensure the security of personal data in accordance with this policy and international information security standards.

The director of BIOIRC DOO may authorize the removal of personal data carriers from the BIOIRC DOO when previously the employee shall enter the purpose and reason for the removal of data from the BIOIRC DOO in the record book on the handling of personal data.

For the purposes of the BIOIRC DOO, the transfer of personal data to authorized external institutions and others that demonstrate a legal basis for obtaining personal data is permitted by the director of BIOIRC DOO.

The forwarding of personal data from the previous paragraph of this article shall be entered in the record book on the handling of personal data.

Article 9 (*Maintenance and repairs*)

Maintenance and repair of computer hardware and other equipment with which personal data is processed is permitted only with the knowledge and approval of the director of BIOIRC DOO or a person authorized by them, and may only be carried out by authorized services and their maintenance personnel, who have concluded an appropriate contract with the institution on the processing of personal

Chapter IV - PROTECTION OF SYSTEM AND APPLICATION SOFTWARE COMPUTER EQUIPMENT AND DATA PROCESSED WITH COMPUTER EQUIPMENT

Article 10 (*Accessing and Modifying the Software*)

Access to computer software must be protected in a way that allows access only to certain authorized workers and workers who perform servicing of computer and software for BIOIRC DOO under a contract on the processing of personal data.

Repairing, changing and supplementing system and application software is permitted only on the basis of general or individual approval of the director of BIOIRC DOO or a person authorized by them and taking into account the existing security policies of BIOIRC DOO, and it can only be carried out by authorized contractors or their employees, who have concluded an appropriate contract with BIOIRC DOO regarding the processing of personal data.

Contractors must properly document changes to system and application software in proportion to the size of the changes and in proportion to the risks to the security of personal data.

Article 11 (*Development and test environments*)

Development and test environments may not contain personal data, but rather anonymized or fictitious data.

The transition from the test to the production environment must be carefully documented. In this case, the inclusion of personal data in the production environment must be carefully controlled. Personal data must not remain uncontrolled at any time or they may not be processed until the production environment meets all the security requirements specified in this policy. Transitions must be appropriately and traceably documented.

Article 12 (*Storage Location*)

Personal data of BIOIRC DOO may only be stored on the server of BIOIRC DOO. Workstations (computers) may store personal data only if it is absolutely necessary for the performance of work.

Notwithstanding the first paragraph of this article, personal data may also be stored outside the BIOIRC DOO server, if the service provider provides at least such processing security measures as those specified in this rulebook and security policies of the BIOIRC DOO and an appropriate contract has been concluded for such data storage or there is another legal basis for it.

All workstations on which personal data are stored must be encrypted. Competent persons, in case of purchasing new software, are obliged to purchase equipment that complies with the provisions of this paragraph. For all existing software that does not comply with the requirement from this paragraph, the competent person must assess the risk of information security and prepare an impact assessment for the protection of personal data.

Article 13 (*Maintenance of workstations*)

The same provisions apply to the storage and protection of application software as to other personal data and the media on which they are located, from these regulations.

An employee authorized to process and handle personal data on a computer must ensure that, in the event of possible copying of personal data, before servicing, repairing, changing or supplementing of system or application software or after the need for a copy ceases, the copy is destroyed.

An employee authorized to process and handle personal data on a computer must be present at all times during the servicing of the computer and software and must supervise that no impermissible handling of personal data occurs.

In the event that there is a need to repair a computer whose disk contains personal data, outside the institution and without the control of an authorized employee of the institution, the data from the computer disk must be deleted in a way that prevents restoration. If such erasure is not possible, the repair must be carried out in the BIOIRC DOO business premises in the presence of an authorized employee.

Article 14 (*Protection of workstations*)

The content of the disks of the network server and local workstations, where personal data is located, is checked for the presence of computer viruses and malicious software in accordance with the checking plan.

When a computer virus or malicious software appears, it is necessary to do everything in accordance with the guidelines, rules of the BIOIRC DOO, and international guidelines on protecting information security, to eliminate the virus with the help of experts and to determine the cause of the appearance of the virus.

All data and software that are intended for use on the BIOIRC DOO computers and in the BIOIRC DOO computer information system and arrive at the BIOIRC DOO on computer data transfer media or via telecommunications channels will be included in the processing of personal data, they must be checked for the presence of computer viruses before use.

Article 15 (*Prohibition of software manipulation*)

Employees may not install software without the express permission of the director of BIOIRC DOO or modify the existing ones outside of normal permissible use.

Article 16 (*Passwords*)

Access to data through application software must be protected by a system of personal passwords or by another approved method for authorization and identification of users of programs and data. Password system or of access must provide information on who and when individual personal data was processed, in systems where this is possible, as well as information on the purpose of processing. The processing data must be recorded in such a way that it is not possible to change the data in the event log (journal, log file). Such data must be complete and authentic.

The director of BIOIRC DOO, on the proposal of the DPO, determines the regime for assigning, storing and changing passwords for all information systems managed by BIOIRC DOO.

The basic rules are:

- any password that is in use in the information system of BIOIRC DOO must be at least 8 characters long and must contain at least one uppercase and lowercase letter, at least one number and at least one special character (e.g. "#%&'() "). The password must not contain names, surnames, known facts or words from any language. The time for periodic password changes is determined in accordance with the identified risks. The new password must not be the same as the user's last five passwords;
- the password is determined by each user himself and must not be disclosed to anyone, including his superiors or system supervisors. Users may not use the same password outside BIOIRC DOO information systems.

When assigning and restricting access to applications and data, the following restrictions must be taken into account:

- users have access only to those applications and data they need to perform their work and order;
- users may not have access to applications and data for which they do not have access rights;
- users must not have access to data/information marked with a level of confidentiality for which they have no authority.

Accesses to applications and data that the user does not need to perform their work and tasks are not permitted, even if the user's access is not restricted.

Users are responsible for all activities that occur with their user identification and password or qualified digital certificate.

Article 17 (*System passwords*)

All system passwords and procedures used for access and administration in the network of personal computers, administration by e-mail and administration via application programs are kept in sealed envelopes in a fireproof cabinet or safe at the BIOIRC DOO.

Protected passwords stored in sealed envelopes may be used in exceptional and urgent cases. Any use the contents of the sealed envelopes are documented.

After using the sealed passwords from the envelopes, all used passwords must be changed to new passwords.

Article 18 (*Backups*)

For the purposes of restoring personal data or the computer system after malfunctions or loss of data for other reasons, the appropriate department or employee, appointed by the director of BIOIRC DOO, must regularly make copies of personal data collections and properly document the making of copies .

Copies from the previous paragraph are kept in places designated for this purpose, which must be fireproof, protected against floods and electromagnetic disturbances, within the prescribed climatic conditions and locked with anti-burglary means. These places must be physically separated from the BIOIRC DOO location, and the physical transfer between the two locations can only be carried out by an authorized person, designated by the director of BIOIRC DOO. At no time during the physical transfer shall such copy remain unattended.

Article 19 (*Protection of archives*)

Premises in which archival material containing personal data are located must comply with applicable internationally recognized standards for the protection of archival material.

Regardless of the previous paragraph, the premises in which archival material with personal data carriers (including physical documents) are located must be at least fire-proof and burglar-proof and physically adequate in such a way as to prevent the destruction of personal data due to floods, spills water or other accidents and environmental influences.

Chapter V - SERVICES PROVIDED BY EXTERNAL LEGAL OR NATURAL PERSONS

Article 20 (*Obligation to sign an agreement on the processing of personal data*)

With any external legal or natural person who performs individual tasks related to processing (i.e. also with inspection) personal data (processor) and has at least access to personal data, a written contract on the processing of personal data is concluded. In such a contract, conditions and measures must also be prescribed to ensure the security of personal data processing, or the processor undertakes to comply with these regulations. The aforementioned also applies to third parties who maintain hardware and software and manufacture and install new hardware or software.

External legal or natural persons may only provide personal data processing services within the scope of the client's authorizations and may not process or otherwise use the data for any other purpose.

An authorized legal or natural person who provides agreed services for the BIOIRC DOO outside the operator's premises must have at least as strict a method of protecting personal data as provided for in these regulations.

Chapter VI - ACCEPTANCE AND TRANSFER OF PERSONAL DATA

Article 21 (*Incoming Mail*)

The employee who is in charge of receiving and recording mail must hand over the mail with personal data directly the individual or the service to which this shipment is addressed.

The employee who is in charge of receiving and recording mail opens and inspects all postal shipments and shipments that arrive at the BIOIRC DOO in another way (they are brought by customers or couriers, with the exception of shipments from the third and fourth paragraphs of this article).

The employee who is in charge of receiving and recording mail shall not open those shipments that are addressed to another authority or organization and have been delivered by mistake, as well as shipments that are marked as personal data or for which it follows from the markings on the envelope that refer to a competition or tender. In the event that the shipment is addressed to another authority or organization and is mistakenly delivered to BIOIRC DOO, the worker in charge of receiving and registering the mail,

will without delay sent to the address authority or organization, subject to the meaningful application of the provisions of the law governing the general administrative procedure.

An employee who is in charge of receiving and recording mail may not open shipments addressed to the employee, on which it is stated on the envelope that they are to be served personally to the addressee, and shipments on which the personal name of the employee is first stated without marking his official position and only then the address of the BIOIRC DOO.

Article 22 (*Transfer of personal data*)

Personal data may be transmitted by information, telecommunications and other means only when procedures and measures are implemented that prevent unauthorized persons from unauthorized processing or familiarization with the content.

Personal data in physical form is sent by registered mail.

The envelope in which personal data is transmitted must be made in such a way that the envelope does not allow the contents of the envelope to be visible in normal light or when the envelopes are illuminated with ordinary light. Also, the envelope must ensure that the opening of the envelope and familiarization with its contents cannot be done without a visible trace of the opening of the envelope.

Special types of personal data (previously sensitive personal data) in physical form are sent to addressees in sealed envelopes by courier or by registered mail. During processing, such data must be specially marked and protected in such a way that unauthorized persons are prevented from accessing them.

Special types of personal data in electronic form may be transmitted via telecommunications networks only if they are specially secured with cryptographic methods and electronic signatures in such a way that the data is unreadable during transmission.

Article 23 (*Behavior when transmitting personal data*)

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

For each transmission of personal data, the external user must submit a written application, which must clearly state the provision of the law authorizing the user to obtain personal data, or must attach a written request to the application or the consent of the individual to whom the data refer.

Every transmission of personal data shall be recorded in the records of transmissions, from which it must be clear which personal data were transmitted, to whom, when and on what legal basis.

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

Reviewing and transcribing (copying) administrative files and giving notices about the progress of the procedure shall be carried out in accordance with the provisions of the law governing the general administrative procedure.

Chapter VII - DATA DELETE

Article 24 (*Erase mode*)

After the retention period has expired or the purpose has expired, personal data is deleted or irretrievably destroyed by the data carriers.

Deletion of personal data on computer media is done in a way, according to a procedure and method that makes it impossible restoring deleted data.

Personal data contained on traditional media (documents, files, register, list) are deleted by destroying the media.

The carriers are physically destroyed (burned, cut up) on the premises of the institute or under the supervision of an authorized employee of the institute at the organization dealing with the destruction of confidential documentation.

Destruction and deletion of personal data shall be carried out by commission. The director of BIOIRC DOO appoints the three members to commission with a permanent mandate, which attends and records every erasure and destruction of personal data carriers with minutes.

Article 25 (*Deletion of auxiliary documentation*)

Auxiliary documentation, drafts, computer products or semi-finished products and templates containing individual personal data must also be deleted and destroyed with all the conscientiousness and care specified by these regulations.

The destruction of personal data on the carriers referred to in the previous paragraph must be carried out fluidly and up-to-date.

Chapter VIII - ACTION ON DISCOVERY OF MISUSE OF PERSONAL DATA OR HACKING OF PERSONAL DATA COLLECTIONS

Article 26 (*Obligation to notify and prevent further damage*)

Employees are obliged to inform the DPO of activities related to the discovery or unauthorized processing of personal data, malicious or unauthorized use, appropriation, modification or damage immediately upon detection of a possible incident or harmful event, which is determined by the director of BIOIRC DOO, and they themselves try to prevent such activity. In doing so, employees must not risk their lives or health.

Article 27 (*Information of the individual*)

If the DPO assesses that it is likely that a breach of personal data protection caused a high risk to the rights and freedoms of individuals, the director of BIOIRC DOO must notify the individual to whom the personal data relates within 24 hours at the latest that there has been a breach of personal data protection.

The message from the previous paragraph must be written in clear and simple language and must contain the following Information:

- a message about the name and contact information of the authorized person for data protection of BIOIRC DOO or other points of contact where more information can be obtained;
- a description of the likely consequences of a breach of personal data protection;
- a description of the measures taken or proposed to be taken by BIOIRC DOO to deal with a breach of personal data protection, as well as measures to mitigate any adverse effects of the breach, if relevant.

The notification to the individual referred to in the first paragraph is not necessary in the following cases:

- the competent department of BIOIRC DOO implemented appropriate technical and organizational protection measures and these measures were used for personal data in relation to which a security breach was committed, in particular measures based on which personal data become unintelligible to anyone who is not authorized to access to them, such as encryption;
- the competent department of BIOIRC DOO has taken subsequent measures to ensure that the high risk to the rights and freedoms of individuals to whom personal data refer, from the first paragraph, will probably no longer materialize;

- in cases where such notification would require a disproportionate effort. In such a case, a public notice shall be published instead or a similar measure shall be implemented, by which the individuals to whom the personal data relate are equally effectively informed.

Chapter IX - RESPONSIBILITY FOR IMPLEMENTING PERSONAL DATA SECURITY MEASURES

Article 28 (*Signature of declaration of familiarity with the rules*)

Before an employee begins work or begins other cooperation with BIOIRC DOO, the employee or the contractor is aware of these rules, and as a rule he also signs a declaration of familiarity. The obligation to comply with these regulations also applies if the individual refuses to sign the statement. A professional employee of the BIOIRC DOO makes a note of the refusal to sign the statement.

The obligation to protect personal data applies permanently, even after the end of employment or cooperation.

Article 29 (*Behaviour in case of suspected misdemeanor or criminal offense*)

If there is a suspicion of a misdemeanor in a specific case, the director of BIOIRC DOO shall notify the Information Commissioner of the Republic of Serbia.

In the event that in a specific case there is a suspicion of the commission of a criminal act, the director of BIOIRC DOO shall notify the Police or the competent prosecutor's office.

Chapter X - RECORD KEEPING

Article 30 (*Record of processing activities*)

BIOIRC DOO is obliged to keep records of personal data processing activities, in accordance with the provisions of Article 30 Regulations. The register is updated on an ongoing basis, but it is obligatory once a year.

Chapter XI - TRANSITIONAL AND FINAL PROVISIONS

Article 31 (*Reconciliation of records of processing activities*)

BIOIRC DOO must specify processing activities in their records within 3 months from the adoption of these regulations, persons responsible for individual collections of personal data or processing processes.

BIOIRC DOO must determine access rights for both physical and electronic forms of collections within a period of 3 months from the adoption of these regulations for each workplace which, due to the nature of its work, may process personal data, or processes.

Article 32 (*Harmonization of contracts on personal data processing*)

BIOIRC DOO must harmonize data processing contracts, declarations, records of processing activities and other possible acts regulated by these regulations.

The BIOIRC DOO must inform all employees and external contractors who carry out personal data processing activities within 1 month of the publication of these regulations.

These regulations enter into force on the fifteenth day after the date of publication on the BIOIRC DOO website.

In Kragujevac, on 1 January 2023

Vice Director of BIOIRC DOO:
prof. dr. Nenad Filipović

ATTACHMENTS:

Annex 1

Employee's statement or the contractor on the security of personal data

I, the undersigned , confirm that I have read the Regulations on the security and processing of the personal data at the BIOIRC DOO, I understand them and undertake to explicitly enforce them throughout my work for the BIOIRC DOO, as well as after I quit my job.

I also confirm that I am familiar with the provisions of the law governing the area of personal data protection and the EU General Regulation on the Protection of Personal Data (GDPR), as well as the consequences of possible non-compliance with the aforementioned rulebook or law or regulation (violation of the employment contract). I am also informed that I will be retroactively liable in the event that the BIOIRC DOO where I am employed will have to pay a fine, penalty or compensation due to illegal interference with the protection of personal data, which I will cause through my actions intentionally or due to gross negligence.

Signature: Date and place:

Annex 2

Declaration of the external contractor on the security of personal data

I, the undersigned , confirm that I have read the Regulations on the security and processing of the personal data at the BIOIRC DOO, I understand them and undertake to explicitly enforce them throughout my work for the BIOIRC DOO, as well as after I quit my job.

I also confirm that I am familiar with the provisions of the law governing the area of personal data protection and the EU General Regulation on the Protection of Personal Data (GDPR), as well as the consequences of possible non-compliance with the aforementioned rulebook or law or regulation (violation of the employment contract). I am also informed that I will be retroactively liable in the event that the BIOIRC DOO where I am employed will have to pay a fine, penalty or compensation due to illegal interference with the protection of personal data, which I will cause through my actions intentionally or due to gross negligence.

Signature: Date and place: