DIRECTIVE ON THE PROTECTION OF NATURALS PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article I. Introductory Statement

This Directive is issued for the purpose of specifying the rights and obligations of the staff of the Institute of Biophysics of the Academy of Sciences of the Czech Republic, v.v.i. in connection with the entry into force of Regulation (EC) No 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/ES (General Regulation on the protection of personal data).

Article II. Definitions

1. For the purposes of this Directive and for the purposes of processing the personal data by IBP, an interpretation of the following terms shall be determined:

IBP = Institute of Biophysics of the Academy of Sciences of the Czech Republic, v.v.i. with its registered office at Královopolská 135, Brno, ZIP code: 612 65

Personal data = any information about an identified or identifiable natural person

Identified person = a natural person specifically identified by the name, surname and date of birth**.**

Identifiable person = a natural person who can be identified directly or indirectly, in particular by reference to a particular identifier such as name, identification number, location data, network identifier or one or more specific physical, physiological, genetic, psychological, economic, cultural or social identity feature of this natural person.

Data subject = Identified or identifiable person.

Processing = any personal data or personal data files operation or set of operations performed with or without the help of automated procedures such as collecting, recording, arranging, structuring, storing, customizing or modifying, searching, viewing, using, accessing by transmission, distribution or any other disclosure, sorting or combining, restriction, deletion or destruction.

Restriction of processing = identification of stored personal data in order to limit their processing in the future.

Profiling = any form of automated personal data processing involving the use thereof in evaluating certain personal aspects relating to a natural person, in particular to analyze or estimate aspects relating to work performance, economic situation, health, personal preferences, interests, reliability, behavior, whereabouts or movement of this person.

Pseudonymization = processing of personal data so that said data can no longer be assigned to a specific data subject without the use of additional information, if the additional information is kept separate and is subject to technical and organizational measures to ensure they will not be assigned to any identifiable or identifiable natural person.

Evidence = any structured set of personal data accessible in accordance with specific criteria, whether centralized, decentralized or functionally or geographically separated.

Recipient = natural or legal person, public authority, agency or other entity to whom personal data are provided.

Consent = any free, specific, informed and unambiguous manifestation of wills by which the data subject gives a declaration or other apparent confirmation of his/her consent to the processing of his/her personal data.

Violation of security = violation of security that leads to accidental or unlawful destruction, loss, alteration or unauthorized provision or disclosure of transmitted, stored or otherwise processed personal data.

Genetic data = personal data relating to inherited or acquired genetic traits of a natural person which provide unique information about physiology or health thereof, resulting in particular from an analysis of a biological sample of the natural person concerned.

Biometric data = personal data resulting from specific technical processing relating to physical or physiological features or personality traits of a natural person that allow or confirm unique identification, such as facial image or dactyloscopic data.

Health status data = personal data concerning the physical or mental health of a natural person, including data on the provision of health services that indicate the health status thereof.

Metadata = data providing information about other data.

Automated processing = processing that involves operations of: a) storing information on data carriers; (b) execution of logical or arithmetic operations with such data, modification, erasure, search or dissemination thereof carried out in whole or in part by automated procedures; c) archiving the information by storing them on archiving storage media and, if necessary, updating the information from the archive media.

Manual processing = any processing except for automated processing (physical form, card file, files).

Article III. Basic principles of personal data processing

1. Any processing of personal data should be carried out in accordance with the principle

of transparency. For natural persons, it should be transparent that personal data concerning them are collected, used, consulted or otherwise processed as well as to what extent these personal data are or will be processed. The Transparency Principle requires all information and communications concerning the processing of personal data to be easily accessible and comprehensible and made available using clear and simple means of language. Natural persons have the right to be informed of the identity of the controller and of the processing purposes and other matters in order to ensure fair and transparent processing in relation to the natural persons concerned and their rights to obtain confirmation and to communicate the personal data processed relating to them. Natural persons should be made aware of the risks, rules, warranties and rights existing in relation to the processing of their personal data and how they should exercise their rights in connection with such processing.

2. Any processing of personal data should be carried out in accordance with the principle of legitimacy. In particular, it is necessary that the specific purposes for which the personal data are processed are unambiguous and legitimate and set out at the time of the collection of personal data.

3. Any processing of personal data should be carried out in accordance with the principle of proportionality. Personal data should be proportionate, relevant and limited to what is necessary for the purposes for which they are processed. In particular, it is necessary to ensure that the period for which personal data are kept is limited to the minimum necessary. Personal data should be processed only if the purpose of processing cannot be reasonably achieved by other means. In order to ensure that personal data are not kept longer than necessary, deletion and review deadlines are set.

4. Any processing of personal data should take place in such a way as to guarantee proper security and confidentiality of such data, inter alia in order to prevent unauthorized access to personal data and to the equipment used to process them or to prevent unauthorized use thereof.

5. Any processing of personal data should take place in a way that guarantees accuracy of the personal data recorded. Inaccurate personal data will be erased or corrected immediately.

6. Any processing of personal data should take place in a safe manner.

7. Storing personal data in a form that allows for identification of data subjects can only take as long as is necessary for the purposes for which the data are processed. This does not apply if personal data are processed solely for the purposes of archiving pursuant to Act No. 499/2004 Coll., On archiving and filing in accordance with Decree No. 259/2012 Coll., On the details of the performance of the filing service and in accordance with IBP Directive No. 10 - Filing and Shredding Rules; for the purposes of scientific or historical research, statistical purposes, provided that all security and technical safeguards are in

place to ensure that personal data cannot be handled otherwise and that all rights and freedoms of data subjects are guaranteed.

8. Any processing of personal data must always take into account specific protection of children's personal data.

9. Personal data of particular sensitivity in terms of fundamental rights and freedoms deserve specific protection. Such personal data include personal data of racial or ethnic origin. Derogations from the general prohibition on the processing of these specific categories of personal data should be expressly provided, inter alia, in case the data subject gives his/her explicit consent or in case of specific needs. Specific categories of personal data deserving a higher level of protection should only be processed for medical and scientific purposes if these purposes are to be achieved for the benefit of natural persons and society as a whole and for archiving purposes pursuant to Act No. 499/2004 Coll., On archiving and filing in accordance with Decree No. 259/2012 Coll., On the details of the performance of the filing service and in accordance with IBP Directive No. 10 - Filing and Shredding Rules.

Article IV. Reasons for processing personal information

1. Processing of personal data may only be conducted for the legal grounds set out in paragraphs 2 to 7 of this Article. The legal grounds for the processing of personal data cannot be extended.

2. Processing of personal data can be done if the data subject has given consent to the processing of his/her personal data for one or more specific purposes. Approval with the processing of personal data is granted in writing and in physical form or in the form of a data message. The data subject must be given the consent to the processing of personal data in a manner that is comprehensible, using clear and simple means of language. The data subject has the right to revoke his/her consent at any time in the same way that the consent was granted, i.e. in writing and in physical form or in the form of a data message.

3. Processing of personal data may be conducted when it is necessary to meet contract requirements to which the data subject is a contracting party or to implement measures taken before the conclusion of the contract at the request of the data subject.

4. Processing of personal data can be done when it is necessary to fulfill the legal obligations of the IBP.

5. Processing of personal data can be done when it is necessary to protect the vital interests of the data subject or other natural person.

6. Processing of personal data can be done when it is necessary to fulfill the public interest task assigned to the IBP.

7. Processing of personal data can be done when it is necessary for the legitimate interests of the IBP or third parties, except in cases where the fundamental rights and freedoms of the data subject that require the protection of personal data are preferred to those of interest, in particular in case the data subject is a child.

Article V. Reasons for processing specific categories of personal data.

1. Processing of personal data that tell of racial and ethnic origin, political opinions, religious beliefs or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of unique identification of a natural person, health status data, sexual life data, and sexual orientation of a natural person data can only be based on the legal grounds set out in paragraphs 2 to 8 of this Article. Processing for other legal reasons is prohibited.

2. Processing of personal data of a specific category is only possible if the data subject has given his/her explicit consent for one or more specified purposes. Approval of the processing of personal data is granted in written form and in physical form. The data subject must be given the consent to the processing of personal data in a manner that is comprehensible, using clear and simple means of language. The intended purpose must be exactly linguistically defined. If possible, the duration of the consent is also defined. This is without prejudice to the right of the data subject to revoke his/her consent at any time, in writing, in physical form or in the form of a data message or in the form of an e-mail.

3. Processing of personal data of a specific category is only possible if such processing is necessary for the fulfillment of obligations and the exercise of specific rights of the IBP in the field of labor law, social security and social protection law.

4. Processing of personal data of a specific category is only possible if the processing is necessary to protect the vital interests of the data subject or other natural person, in case the data subject is not physically or legally authorized to grant consent.

5. Processing of personal data of a specific category is only possible if the processing concerns personal data clearly disclosed by the data subject.

6. Processing of personal data of a specific category is only possible if the processing is necessary for the purposes of archiving in the public interest, for the purposes of scientific or historical research, or for statistical purposes.

7. Processing of personal data of a specific category is only possible if the processing is necessary for the purposes of preventive medicine, for assessment of the Employee's ability to work, medical diagnostics, provision of health or social care, treatment.

8. Processing of personal data of a specific category is only possible if the processing is necessary for reasons of public interest in the field of public health such as the protection against serious cross-border health threats or the provision of strict quality and safety standards for health care and for medicinal products or medical devices.

Article VI. Saving personal data

1. IBP stores personal data in a physical (analog) and electronic (digital) form. IBP has a physical repository in the framework of IBP agenda execution, a document repository within internal organization, a file service information system, its own agenda information systems, third party information systems, an economic information system, portals, other electronic repositories.

2. The IBP agenda performance physical repository includes all the documents that are stored in the organization and are related to the performance of the agendas of the organization.

3. The IBP internal organization operation physical repository includes all the documents that are stored in the organization and are related to the internal operation of the organization, in particular questions of job applicants, Employees, other personnel agenda, accounting, etc.

4. The file service information system is an electronic repository which contains an electronic filing system agenda in accordance with Act No. 499/2004 Coll., On archiving and filing in accordance with Decree No. 259/2012 Coll., On the details of the performance of the filing service, and in accordance with IBP Directive No. 10 - Filing and Shredding Rules.

5. Own agenda information systems are electronic repositories that contain central data repositories, including scientific and human resources repositories, application and computing servers, LDAP database of institutional services users, as well as system backups of the data warehouse server and server backups and user data backups. These include, for example, FILES REPOSITORIES located on the intranet, CESNET File Sender, JAVOR data store, local DNS server.

6. Third party agenda information systems are electronic repositories that contain data repositories for scientific activities carried out in cooperation with a third party, usually with healthcare facilities (specifically hospitals) and universities (specifically science and medical faculties).

7. The economic information system is an electronic repository that contains data related to bookkeeping, accounting, reporting, budgeting, etc.

8. Portals (public and non-public web portals) are electronic repositories that contain IBP web presentations and intranet sites.

9. Other electronic repositories are electronic repositories, such as emails (a web-based email interface including a directory, calendar, notes, tasks), shared drives, local disks on computer assemblies, and so on.

10. The manner of storing personal data, which is not explicitly mentioned here, is governed by the IBP Internal Directive No. 10 - Filing and Shredding Rules.

Article VII. Processing of personal data of job applicants

1. IBP processes personal data of IBP job applicants for negotiations of the conclusion of an employment contract or agreements on work activities or employment agreements, carried out based on the proposal of the data subject (application to the selection procedure).

2. IBP usually processes the following personal data: - name and surname, date of birth, achieved education, previous work experience and professional traineeships.

3. Personal data of the IBP job applicants will be destroyed by IBP immediately after the end of the selection process by shredding personal data communicated in a written (analog) form and removing irrevocably personal data communicated in digital form from all of its facilities. The IBP job applicant has the possibility to grant IBP consent to the processing of his/her personal data necessary for the negotiations of a contract of employment solely for the possibility of reaching the job applicant in case of a further selection procedure for a similar position the job applicant was originally interested in. Such consent to the processing of personal data is granted only for a limited period of time, at most 10 (ten) years.

Article VIII. Processing of personal data of Employees

1. IBP processes the personal data of its Employees. For the purposes of this Directive, the person who performs any activity for IBP on the basis of an agreement on work activity and employment agreement is considered to be an Employee.

2. IBP processes the following personal data on the basis of legal regulations:

name and surname,
date of birth and national identification number,
citizenship,
address of permanent residence / address of permanent residence of foreigners,
achieved education, previous experience,
details of the receipt of old age or disability or orphan pension,
for female Employees, the number of children,

health disabilities,
health insurance company with which the Employee is insured.

3. The legal regulations on the basis of which the Employer processes personal data are:
Act No. 262/2006 Coll., Labor Code,
Act No. 280/2009 Coll., Tax Code,
Act No. 586/1992 Coll., on Income Tax,
Act No. 563/1991 Coll., on Accounting,
Act No. 582/1991 Coll., on the Organization and Implementation of Social Security,
Act No. 187/2006 Coll., on Sickness Insurance,
Act No. 435/2004 Coll., on Employment,
Act No. 48/1997 Coll., on Public Health Insurance.

4. In case the Employee applies a tax benefit to a spouse pursuant to § 35c paragraph 8 of Act No. 586/1992 Coll., on income tax, the Employer processes personal data consisting of the name and surname of the spouse and the name and registered office of his/her Employer.

5. In case the Employee applies a tax benefit to a dependent child pursuant § 35c paragraph 1 of Act No. 586/1992 Coll., the income tax, the Employer processes personal data consisting of the name, surname and national identification number of the child.

6. Each Employee receives written information about the processing of personal data under statutory regulations, as specified in this Article in paragraph 2, upon concluding an employment contract, employment agreement or work activity agreement.

7. IBP publishes on its website only the name and surname of the Employees who are employed at such positions which assume negotiations or some other way of cooperating of said Employees with the public. For these Employees, their work e-mail address, telephone number and job position are also published.

8. The Employee has the opportunity to grant the Employer consent to process personal data, consisting of a bank account number, to pay the wage or remuneration from an employment agreement or work activity agreement.

9. The Employee has the opportunity to grant the Employer consent to process personal data, consisting of his/her telephone number, e-mail address, data box ID, correspondence address, to facilitate mutual communication between the Employee and the Employer.

10. The Employee has the opportunity to grant the Employer consent to process personal data, consisting of his/her first name and surname, for the purpose of Employee catering provided directly by IBP.

11. The Employee has the opportunity to grant the Employer consent to process personal data and to publish the personal data on IBP websites, consisting of his/her name and surname, image, achieved education, work experience, etc. With no consent, IBP only publishes names and surnames of the Employees who are employed at such positions that assume negotiations or some other way of cooperating of said Employees with the public. For these Employees, their work e-mail address, telephone number and job position are also published.

12. The Employee has the opportunity to grant the Employer consent to process personal data consisting of the license plate or RN of his/her personal car, for the purpose of enabling his/her personal car to be parked on the premises of IBP.

13. The Employee has the opportunity to grant the Employer consent to process other personal data, to process personal data for other reasons. The provision of other personal data must be linked to the definition of the purpose for which such further personal data will be processed.

14. The data addressed in this Article in paragraph 2 or in paragraphs 3 - 13, respectively, shall be recorded in the personal file of the Employee. The personal file can be accessed by senior employees who are superior to the Employee concerned. The personal file can be accessed by Labor Inspection Authority, the Labor Office of the Czech Republic, and the Office for Personal Data Protection, the court, the public prosecutor, the police body, the National Security Office and the intelligence services. Submission of individual documents by the Employer from said file to an external controlling body which carries out an inspection with the Employer and which requested said document in connection with the subject of an inspection carried out with the Employer is not considered to be an access to the personal file. The Employee has the right to inspect his/her personal file at any time, to make excerpts and to make copies of the documents contained therein, at the expense of the Employer.

15. Employees have the same rights as third parties, as specified in Article X.

Article IX. Processing of personal data of contractual partners

1. IBP processes the personal data of contractual partners necessary for the performance of contracts to which the data subject is a contracting party or to implement measures taken before the conclusion of the contract at the request of the data subject. The personal data processed by IBP usually consist of the name and surname, date of birth, national identification number, home address, delivery address, identification number, tax identification number, bank account number.

Article X. Processing of personal data of third parties

1. IBP processes the personal data and specific category personal data of third parties,

particularly on the basis of their consent. Processing of personal data can be done if the data subject has given consent to the processing of personal data for one or more specific purposes. Consent of the processing of personal data is granted in writing and in physical form or in the form of a data message. The data subject must be given the consent to the processing of personal data in a manner that is comprehensible, using clear and simple means of language. Processing of personal data of a specific category is only possible if the data subject has given his/her explicit consent for one or more specified purposes. Approval of the processing of personal data is granted in written form and in physical form. The data subject must be given the consent to the processing of personal data in a manner that is comprehensible, using clear and simple means of language. The intended purpose must be strictly linguistically defined. If possible, the duration of the consent is also defined.

2. The data subject has the right to revoke his/her consent at any time. Revocation of consent is without prejudice to the lawfulness of processing based on consent given prior to the revocation thereof. Even upon revocation of consent, IBP may process personal data and specific categories of personal data, if necessary, for archiving in the public interest, for scientific and historical research purposes or for statistical purposes; provided that fundamental rights and interests of data subjects are investigated. Revocation of consent to the processing of personal data is done in written form, in physical form, in the form of a data message or in the form of an e-mail. Revocation of consent to the processing of personal data of a specific category shall take place in oral form, in person or by telephone, or in written form in the form of a data message or in the form of an e-mail.

3. The data subject has the right to obtain from IBP a confirmation that the personal data concerning him/her are processed or not and, if so, he/she has the right to access these personal data and the following information: purpose of processing, category of personal data concerned and specific categories of personal data, recipients or categories of recipients to whom personal data have been or will be made available, in particular recipients in third countries or international organizations, the envisaged period for which personal data will be stored or, if it is not possible to determine the period, the criteria used to determine said period, the existence of the right to require the controller to rectify or delete personal data relating to the data subject or to restrict their processing, or to object to such processing, the right to file a complaint with the supervisory authority, any available information on the source of personal data, if not obtained from the data subject. The confirmation under paragraph 4 of this IBP article is provided in the form, scheme, formats and language relative to the content of the confirmation, including its metadata. IBP is not obliged to change the confirmation format or language, nor to create metadata for confirmation, if such a change or creation of metadata would be an unreasonable burden for IBP; in this case, the IBP will comply the request by providing a confirmation in the form, scheme, format or language in which it was created.

4. IBP will provide a copy of the personal data processed at the data subject's request.

The copy of processed IBP personal data is provided in a form, scheme and formats and languages, relative to the content of the request for confirmation, including metadata related to it. IBP s not obliged to change the confirmation format or language, nor to create metadata for confirmation, if such a change or creation of metadata would be an unreasonable burden for IBP; in this case, the IBP will comply the request by providing a confirmation in the form, scheme, format or language in which it was created. The right to obtain a copy must not adversely affect the rights and freedoms of other third parties.

5. The data subject has the right that IBP corrects, without undue delay, any inaccurate personal data relating to the data subject. As a rule, IBP will correct inaccurate personal data within ten (10) days of receipt of the request for personal data repairs. The request for correction of personal data is filed with the IBP in physical form, in the form of a data message or in the form of an e-mail. Due to the purpose of processing, the data subject has the right to supplement incomplete personal data, inter alia by providing additional consent.

6. The data subject has the right to request IBP to erase, without undue delay, personal data relating the data subject. IBP will erase personal data of the requesting data subject if at least one of the following reasons is provided: personal data are no longer needed for the purposes for which they were collected or processed, the data subject revokes processing consent and there is no other reason for which IBP could process the data, subject opposes processing and there are no prevailing legitimate reasons for further processing, personal data have been processed unlawfully, personal data must be erased to fulfill a legal obligation under public law.

Article XI. Processing of personal data in proceedings pursuant to Act No. 134/2016 Coll., On Public Procurement

1. IBP is a contracting authority in accordance with the provisions of § 4 of Act No. 134/2016 Coll., On Public Procurement.

2. IBP in connection with the fulfillment of obligations under Act No. 134/2016 Coll., On Public Procurement, processes personal data. IBP processes personal data only to the extent necessary for the lawful award of lawful public procurement, always taking into account the specific public procurement.

3. IBP is required, in accordance with § 216 para. 1 of Act No. 134/2016 on Public Procurement, to keep a documentation on the tender procedure consisting of all documents in physical or electronic form and oral communication outputs, the acquisition of which during the tender procedure, if necessary after its termination, is required in accordance with Act No. 134/2016 On public procurement, including the full text of the originals of the tenders of all suppliers, for a period of 10 years from the date of termination of the tender procedure or from a change of the contract's commitment to the public procurement.

Article XII. Processing of personal data in order to obtain targeted support for research projects

1. IBP receives targeted support for basic research projects from the Grant Agency of the Czech Republic (hereinafter referred to as the "GA CR"). In order to receive support from the GA CR, IBP processes personal data of its Employees and third parties (employees of collaborating scientific institutions).

2. In order to obtain support for basic research projects, IBP processes and the Czech Science Foundation provides personal data of Employees and third parties (employees of cooperating scientific institutions) consisting of the name, surname, date of birth, national identification number, work telephone number, work e-mail address, citizenship, employer data, i.e. the name, registered office and company ID, type of workload, requested payroll amount.

3. For the purpose of obtaining support for basic research projects, IBP processes personal data of its Employees and third parties (employees of the cooperating scientific institutions) based on the legitimate interest of IBP.

Article XII. Processing of personal data of patients

1. IBP in the public interest collaborates on research activities with healthcare facilities (especially hospitals) and universities (in particular science and medical faculties). For this purpose, IBP is provided with biological material that contains genetic data, biometric data, and health status data. This biological material is processed by the DCBR Department of Radiology and Cell Biology and DC - Cytokinetics.

2. IBP only receives anonymized numbered samples of biological material from medical facilities and universities. IBP does not accept samples of biological material in a form other than anonymized.

3. If necessary for research purposes, IBP receives samples of biological material in pseudonymized form. Pseudonymization takes place in a way that IBP receives samples of biological material labeled with numbers. Independently of receiving samples of biological material labeled with numbers, IBP is provided or sent a document containing the assignment of patients' personal data to sample numbers. Said data consist of the name, surname, diagnosis of the disease, staging (determining the extent of tumors), grading (grading the microscopic degree of differentiation - the maturity of the tumor). A document containing the assignment of patients' personal data to the sample numbers is forwarded either personally to the person authorized by IBP to receive the document or is sent to this person by registered mail or e-mail in the form of a document being encrypted, provided that the document password is communicated to the person authorized by another means of communication, such as in person, by phone, SMS, etc.

4. A document containing the assignment of patients' personal data to sample numbers of the biological material is kept in a physical form by the person authorized in a locked case, in a locked office (see Article XII paragraph 3) or in electronic form in such a way that the document is always encrypted and is stored so that only an authorized person can access it.

Article XIV. Handling of personal data by IBP Employees

1. Employees are bound by all the rules and principles of processing personal data under this Directive.

2. IBP continuously checks whether the rules and principles of the processing of personal data set out in this Directive are properly respected its Employees. To this end, IBP monitors compliance with the rules and principles of personal data processing, inter alia, monitors all repositories (both physical and electronic), including monitoring the use of the Internet network.

3. Employees are required to handle personal data in accordance with the principles of legality, fairness, and transparency. Employees have an obligation to protect the confidentiality of information they use or process in their activities.

4. Employees are required to collect and process personal data only for the fulfillment of their employment obligations and only if these are strictly necessary for the performance of their duties. Employees are required to collect and process personal data in accordance with the "need to know" principle.

5. Employees are required to keep documents containing personal data in designated lockable cabinets in designated offices. If the Employee leaves the office, he/she is required to check and ensure that documents containing personal data are not freely placed in the office but are stored and locked in the designated ward unless another authorized employee works with them. If there is no other employee in the office, the Employee is also required to lock the office.

6. Documents containing personal data that the Employee no longer needs to fulfill his/her duties are required to be handed over by the Employee to the person responsible for the filing service (the employee responsible of the director's secretariat) who places them in the archive. The archive is located in the room number 29. If such a document is part of the file, the Employee is obliged to hand over the document for archiving as part of the file only if he/she does not need the complete file in order to complete his/her work duties.

7. If an Employee uses a computer (desktop, laptop, etc.) for his/her work, he/she is required to log in to the operating system by his/her name and password. The password is chosen by the Employee himself/herself, wherein the password must be at least 9

characters, it must contain capital letters, lower case letters, and digits. Every computer must have an active antivirus and antispam. If an Employee detects that the antivirus or antispam on the computer is missing or not current, he/she is required to notify the IT department. If an Employee leaves the workstation where his/her computer is located, he/she is required to logout from the operating system. Employee must not share his/her credentials with another person. If an Employee leaves the office with his/her place of work and there is no other employee in the office, the Employee is obliged to lock the office. If an Employee interrupts work for a longer period of time (especially between individual working days), he/she is required to shut down the computer.

8. When an employee uses a laptop computer for his/her work and, in the course of carrying out a work assignment, takes the laptop out of the office designed for placement thereof, or outside the premises of IBP, he/she is required to use a laptop that is encrypted. At the same time, he/she is required to increase supervision over said laptop.

9. Employees are only required to enter IBP electronic repositories under their own names and passwords. A password is chosen by the Employees themselves, wherein the password must be at least 9 characters, it must contain capital letters, lower case letters, and digits. Employees must not share their credentials with another person. Employees are allowed to log into electronic repositories only using devices specially designated for this purpose by IBP. If an Employee has no other instruction from IBP, he/she may enter IBP electronic repositories only from IBP-owned devices that were handed over to them by IBP in order to perform their work duties.

10. IBP assigns each Employee with an e-mail address and an e-mailbox (hereinafter referred to as "work e-mail"). Employees are required to use only said assigned work email to communicate in the course of their work responsibilities. Employee work e-mail is encrypted. The password is chosen by the employee himself/herself, wherein the password must be at least 9 characters, it must contain capital letters, lower case letters, and digits. Employees are only allowed log into their work e-mails from devices specially designated for this purpose by IBP. If an Employee does not have a different instruction from the IBP, he/she may log into his/her work email only from a device that is owned by IBP and was handed over to him/her by IBP in order to perform his/her work duties.

11. If Employees send an e-mail that includes an attached attachment containing personal data, they are required to encrypt the attachment containing personal data. The password for the decryption of the attachment is provided by the Employee to the e-mail addressee by another communication path (by phone, SMS, in person). It is forbidden to place personal data of third parties directly in the text of the e-mail. The details of the encryption are governed by the instructions of the IT department.

12. It is forbidden to use the so-called freemail accounts of hosted mail servers that provide email to all interested parties free of charge (for example: email.cz, seznam.cz, gmail.com, yahoo.com, etc.).

13. It is forbidden to use communication paths - multiplatform instant messaging applications such as Skype, WhatsApp, Facebook, Viber, etc. to send documents that contain personal data.

14. Employees are entitled to use the Internet only for the purpose of performing their work duties. It is forbidden to access websites where there is a risk of illegal content (child pornography, sites promoting forbidden ideologies, etc.) or malware (pornography). Also, access to websites where it is possible to share, publish or share files is prohibited, unless it is necessary to perform work tasks (such as facebook.com, uloz.to, youtube.com, etc.).

15. Mobile phones used by Employees to perform their work duties must be encrypted. Access to a mobile phone must be protected by password or similar contemporary technology. SIM cards must be PIN protected. Mobile phones must have automatic keypad locks in case they are not operated for more than one (1) minute. In the absence of a mobile phone provided to an employee by IBP, the employee is not authorized to download any IBP data containing personal data such as e-mail, calendar, contacts, etc. into their mobile phone.

16. Employees are entitled to use USB drives and USB ports only to perform work tasks. Employees are only allowed to use USB discs designated by IBP. If an employee does not have any other instruction from the IBP, he/she may only use USB drives owned by IBP and handed over to him/her by IBP to fulfill his/her work duties. It is forbidden to bring USB drives out of IBP. If it is necessary to bring a USB disk outside IBP to fulfill a work task, the Employee is required to use a USB disk that is encrypted for this purpose. The password is chosen by the Employee himself/herself, wherein the password must be at least 9 characters, it must contain capital letters, lower case letters, and digits. Employees are only allowed to connect devices specifically designated by IBS to USB ports. If an Employee does not have a different instruction from IBP, he/she can only connect to the USB ports such devices are owned by IBP and were handed over to him/her by IBP in order to perform his/her work duties.

17. If an Employee uses remote access to IBP network, he/she is required to implement it using VPN technology or encrypted RDP protocol. To use remote access to IBP network, the Employee must have an explicit IBP authorization. For remote access to IBP network, the employee uses his/her name and password. The password is chosen by the employee himself/herself, wherein the password must be at least 9 characters, it must contain capital letters, lower case letters, and digits.

18. An Employee is obliged to ensure that no other person that, is not entitled to access personal data, can access such personal data the Employee is working with in the course of his/her work, such as by viewing documents that contain personal data, allowing any access to electronic repositories under the Employee's name and password, etc. The Employee must not leave documents and electronic data repositories unattended.

Article XV. The procedure for data leakage containing personal data

1. If an Employee detects a personal data breach or himself/herself inflicts such a personal data breach, he/she shall immediately report this fact to the authorized person in IBP, which is the IBP Director. The Director is obliged to evaluate the hazards, to ensure all necessary technical and organizational measures leading to correction and to inform the Data Protection Officer, which is the Office of the AS CR, with its registered office at Národní 3, 117 20, Prague 1, ID: 60165171, at the e-mail address poverenec@ssc.cas.cz (hereinafter referred to as the "Data Protection Officer"). The Data Protection Officer is obliged to communicate with the Supervisory Authority, which is the Office for Personal Data Protection.

2. A written statement of notification shall be made by the Employee, including a detailed description of the nature of the personal data breach.

Article XVI. Final provisions

1. This Directive on the protection of natural persons with regard to the processing of personal data comes into effect on 25 May 2018.

In Brno, on 24 May 2018

Assoc. prof. RNDr. Eva Bártová, Ph.D.
Director of the Biophysical Institute
of the Academy of Sciences of the Czech Republic, v.v.i.