Pursuant to Article 64 of the Statutes of the University of Ljubljana (*Uradni list Republike Slovenije* [Official Gazette of the Republic of Slovenia] (hereinafter: UL RS), No. 4/17, with amendments) and pursuant to Article 32 (and on) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (OJ L 119, 4 May 2016, pp. 1—88, hereinafter: the Regulation), the Governing Board of the University of Ljubljana adopted, at its session of 2 April 2020, the following

R U L E S
on the secure processing of personal data at the University of Ljubljana

Chapter I
GENERAL PROVISIONS

Article 1
(Scope of the Rules)

(1) The University of Ljubljana (hereinafter: the UL), carries out educational, research, development and artistic activity through its member faculties, as well as basic, developmental and applied research. In all of these instances, the UL acts as the personal data controller.

(2) These Rules determine the organisational, technical and logical-technical procedures and measures for the security of personal data at the Rectorate and bodies of the University of Ljubljana (hereinafter: the UL) and individual UL member faculties (hereinafter: the member faculty) in order to prevent accidental or intentional unauthorised processing, alteration or loss of personal data, as well as unauthorised access or loss thereof.

(3) Employees and external associates (e.g., research, professional and technical staff and associates, and members of the bodies of the University and member faculties) who process personal data in the course of their work shall be familiar with the provisions of the Regulation, the act governing personal data protection, the sectoral legislation governing the specific area of their work and the content of these Rules.

Article 2
(Meaning of terms)

(1) The terms used in these Rules shall have the same meanings as ascribed to them in Article 4 of the Regulation:
(2) "Personal data carriers" are paper or electronic documents, hard discs, electronic portable storage devices (e.g., USB, portable data units), software and other media on which personal data may be recorded and stored.
(3) "A workstation" is a computer, laptop, tablet or any other similar device that enables not only data recording and storage, but also other types of personal data processing (e.g. display).
(4) "A password" is a series of characters comprising letters, numbers and other characters, and is based on the fact that it is secret and only known to the user.
(5) "A contractor" shall mean an individual or a company responsible and in charge of assigning and restricting access rights to applications and data of the personal data controller and to other information systems.

Chapter II

DATA PROTECTION OFFICER

Article 3
(Appointment of a Data Protection Officer)

(1) At the proposal of the UL Secretary General, the Rector shall appoint a UL Data Protection Officer (hereinafter: the UL DPO).
(2) The UL member faculties may appoint their own DPO if they process larger quantities of personal data or special categories of personal data, or if they estimate based on a risk assessment that they need one. In such a case, the member faculty's Dean shall appoint a person who will be authorised to work directly with the UL DPO (DPO *of the member faculty).*
(3) If a member faculty does not have its own DPO, it shall appoint a contact person who is to coordinate activities relating to personal data protection and collaborate with the UL DPO *(Personal Data Protection Coordinator).*
(4) A person meeting the conditions set forth in the Regulation or the act governing personal data protection may be appointed the UL DPO or DPO of the member faculty; above all, such a person shall have experience in personal data protection, and it is also recommended that they be experienced in information systems security.
(5) If an external natural person or legal entity is appointed to act as the UL DPO, such a person/entity shall ensure that the tasks of the UL DPO are performed directly by the natural persons that meet the conditions stipulated in the fourth paragraph of this article.

Article 4
(Tasks and position of the DPO)

(1) The UL DPO shall perform the following for the UL (the Rectorate):
- tasks stipulated by the Regulation and the act governing personal data protection,
- work coordination and making sure the practice of the DPOs of member faculties is uniform, especially by advising, educating and monitoring the work of the DPOs of member faculties,
- an annual work plan based on the risk assessment and submission thereof to the Rector,
- annual reporting on their work to the Rector.

(2) The DPO of a member faculty shall perform the tasks stipulated by the Regulation and the act governing personal data protection, as well as by the internal rules, for the member faculty's Dean's Office and bodies of the member faculty for which the DPO has been appointed, and especially:
- advise the research and professional-technical staff of the member faculty on questions for which a unified practice of the DPOs of member faculties has been established;
- monitor compliance in personal data protection at the member faculty and report to the UL DPO thereon;
- carry out tasks as authorised by the UL DPO;
- attend college meetings convened by the UL DPO.

(3) The Personal Data Protection Coordinator at a member faculty shall work with the UL DPO, implement measures based on the UL DPO's suggestions, organise employee trainings and inform the employees about handling personal data, and provide the UL DPO with information on any breaches detected.

(4) The UL DPO and a member faculty's DPO shall not be dismissed or penalised for performing their tasks.

(5) The UL DPO shall be provided with access to personal data and processing operations carried out by the University of Ljubljana and a UL member faculty. A member faculty's DPO shall be provided with access to personal data and processing operations carried out by the member faculty for which the DPO had been appointed. For each instance of access, or several instances thereof, an authorisation for consultation shall be provided in accordance with this paragraph based on the purpose of processing and in accordance with the information security policy as well as pursuant to the legal basis.

Article 5
(DPO's contact details)

(1) The Rectorate shall provide the Information Commissioner of the Republic of Slovenia with details of the UL DPO as required by the Regulation and the act governing personal data protection.

(2) On the UL website, the Rectorate shall publish the name, surname and contact details of the UL DPO, as well as the contact details of all DPOs of member faculties. On the member faculty's website, the Dean's Office shall publish the name, surname and contact details of the UL DPO as well as the contact details of the member faculty's DPO who was appointed for said member faculty.

Chapter II:
PROTECTION OF PREMISES AND HARDWARE

Article 6
(Safeguarding the premises)

(1) The premises on which secured personal data carriers, hardware and software are kept (hereinafter: secured premises) shall be protected by organisational, physical and technical measures that prevent unauthorised persons from accessing the data.

(2) Persons who are not employees may not enter secured premises (secretariat, HR office, counselling service office, wages department, passive archives) without accompaniment or the presence of an employee. Those working on secured premises shall oversee the premises conscientiously and diligently, and lock the premises upon leaving them.

(3) The personnel maintaining the premises and other equipment on secured premises, business partners and other visitors may only move around secured premises when accompanied by the institution's employee.

(4) Technical and maintenance personnel and cleaners may move around secured premises outside working hours and without the presence of a responsible worker only if data carriers are stored in locked cabinets and workstations are locked in the manner set out in these Rules for the period outside working hours.

(5) Access to the premises referred to in the first paragraph of this article shall be possible and permissible only during working hours, and outside working hours only on the basis of an authorisation from the Secretary General and a member faculty's secretary at the member faculty.

(6) Personal data carriers stored outside active work premises or outside secured premises (hallways, common areas, active and passive archives, etc.) shall be permanently locked in a secure, fireproof cabinet.

(7) The keys to the secured premises shall be kept on the premises designated by the UL house rules and the house rules of member faculties, whereas any unusable keys shall be destroyed on the decision and under the supervision of a commission. Keys shall not be left in locks on the outside of doors.

(8) Secured premises may not be left unsupervised, and shall be locked during any absence of the workers that oversee them.

Article 7
(Data carrier handling)

(1) Personal data carriers shall be kept on secured work premises outside working hours.

(2) Outside working hours, computers and other hardware on which personal data is processed or stored shall be switched off and physically secured or secured by means of software, and access to the personal data stored in workstations shall be encoded.
(3) The computers that need to be switched on all the time to ensure continuous access shall be secured in the sense of the first paragraph of Article 6.
(4) Employees may not leave personal data carriers (including documents) on desks in the presence of persons who do not have the right to consult them (e.g., customers). Anytime an employee leaves their work post, they shall ensure that no personal data is left on their desk or any other work surface (clean desk policy), which includes any personal data filing system carriers; the workstation (computer) shall be locked by means of software or switched off (clear screen policy).
(5) On the premises that may be accessed by customers or persons not employed by the institution, data carriers and computer displays shall be set up so as to prevent such persons viewing them during processing or work on them.
(6) Data carriers that contain special categories of personal data shall be specially marked and secured.

Article 8
(Processing premises)

(1) Personal data from personal data filing systems may only be processed on the institution's premises. The institution's workers may not take any personal data carriers outside the institution.
(2) An exception from the provision referred to in the first paragraph of this article shall be allowed if taking the data carrier out and/or processing of personal data outside the institution is explicitly allowed by the UL Secretary General beforehand, or, in the case of data kept at a member faculty, the secretary of said member faculty. When an employee takes data carriers and/or processes personal data outside the secured premises, they shall ensure personal data is secured in accordance with these Rules and international information security standards.
(3) The UL's Secretary General or a member faculty's secretary may permit taking personal data carriers outside the institution once the worker first enters the purpose and reason for taking the data outside the institution in the Register of Records of the Handling of Personal Data.
(4) The transmission of personal data to authorised external institutions and others who demonstrate a legal basis for obtaining personal data shall be permitted, for the purposes of the University of Ljubljana, by the UL's Secretary General and, for a member faculty, by the faculty secretary.
(5) Transmission of personal data as referred to in the preceding paragraph of this article shall be entered in the Register of Records of the Handling of Personal Data or automatically in the audit trail.

Article 9
(Maintenance and repairs)

(1) The maintenance and repair of computer hardware and other equipment used to process personal data shall be permitted only with the knowledge and upon approval of the UL's Secretary General or a member faculty secretary or a person authorised by them, and may only be carried out by the authorised servicer and their maintenance staff who have concluded an appropriate personal data processing contract with the institution.

Chapter III:
PROTECTION OF SYSTEM AND APPLICATION SOFTWARE, AND OF COMPUTER-PROCESSED DATA

Article 10
(Access to and modification of software)

(1) Access to software shall be secured in such a way as to permit access solely to certain authorised workers and to persons who service hardware and software for the UL or a member faculty under the personal data processing contract.
(2) Correcting, modifying and updating system and application software shall only be permitted based on a general or individual approval provided by the Secretary General or a member faculty secretary or by a person authorised by them, and, taking the existing security policies of the UL into consideration, may only be performed by authorised service providers or their employees who have signed the relevant contract on personal data processing with the UL or a member faculty.
(3) Service providers shall appropriately document modifications to system and application software in proportion with the scope of modifications and with personal data security risks.

Article 11
(Development and testing environment)

(1) Development and testing environments may not contain any personal data; instead, the data shall be rendered anonymous or fictitious.
(2) Transition from the testing environment to the production environment shall be carefully documented. In this process, incorporation of personal data in the production environment needs to be monitored with care. Personal data may at no point remain unsupervised, i.e., it may only be processed once the production environment provides all the security requirements set forth in these Rules. Transitions shall be documented in a way that is appropriate and traceable.

Article 12
(Storage location)

(1) The personal data of the UL and of member faculties may only be stored on the UL or member faculty's server. Personal data may only be kept on workstations (computers) if this is absolutely necessary to perform the work.
(2) Regardless of the first paragraph of this article, personal data may also be kept outside the UL's or member faculty's server if the service provider ensures at least the processing security measures set forth by these Rules and the UL's security policies, and if an appropriate contract has been concluded for such data storage or if there exists any other legal basis for it.
(3) All workstations on which personal data is stored shall be encrypted. In the event of purchasing new software, the competent persons shall be obliged to purchase software that is compliant with the provisions of this paragraph. For all the existing software that is not compliant with the requirement from this paragraph, the competent person shall assess the risk to information security and prepare an assessment of effects on personal data protection.

Article 13
(Workstation maintenance)

(1) As regards the storage and security of application software, the same provisions from these Rules shall apply as to other personal data and carriers on which they are stored.
(2) The worker authorised to process and handle personal data on a computer shall ensure that any copies of personal data made before the servicing, repair, modification or updating of system or application software are destroyed as soon as the copies are no longer required.
(3) The worker authorised to process and handle personal data on a computer shall be present throughout the computer and software servicing operation, and shall supervise the process to ensure that no unauthorised handling of personal data takes place.
(4) Where the need arises for repair work outside the institution's premises and without supervision by the authorised worker of the institution, on a computer on which personal data is stored, personal data shall be deleted from the computer disc in such a way that it cannot be restored. If such deletion is not possible, the repair work shall be performed on the institution's premises and in the presence of the authorised worker.

Article 14
(Workstation protection)

(1) The content of network server discs and of local workstations on which personal data is located shall be checked for computer viruses and malware in accordance with the verification plan.
(2) Upon the appearance of a computer virus or malware, everything shall be done in line with the guidelines, rules of the member faculties and of the UL, and international guidelines on information security protection, to remove the virus with the help of experts and to establish the reason for its occurrence.
(3) All data and software intended for use on the institution's computers and within the institution's computer information system and that arrive to the institution on media used for the transfer of computerised data, or via telecommunications channels, and are or will be included in personal data processing shall be checked for the presence of computer viruses prior to use.

Article 15
(Prohibition of software manipulation)

(1) Employees may not install software or modify the existing software beyond usual permissible use without the explicit permission of the Secretary General or a member faculty's secretary.

Article 16
(Passwords)

(1) Access to data via application software shall be secured by means of a system of personal passwords or another approved method for authorising and identifying software and data users. The system of passwords/access shall provide the information on who processed an individual piece of personal data and when, as well as information on the purpose of processing in the systems where this is possible. The information on processing shall be recorded in a manner that makes changing data in the event log (journal, *log file)* impossible. Such data shall be comprehensive and authentic.
(2) At the proposal of the UL IT Department, the Secretary General shall determine the regime of assigning, storing and changing passwords for all information systems managed by the UL.
(3) The basic rules are as follows:
Any password used in the information system of the UL or a member faculty, shall be at least 8 characters long, and shall contain at least one lower case and one upper case letter, at least one number and at least one special character (e.g., »#%&'()«). A password may not contain names, surnames, known facts or words from any language. The time for a periodic password change shall be determined in line with the risks identified. The new password may not be the same as any of the user's previous five passwords. Every user shall create their own password and may not disclose it to anyone, not even their superiors or system supervisors. Users may not use the same password outside the UL's information systems.

(4) The following restrictions shall be considered when assigning and restricting access to applications and data:
- users may have access only to those applications and data which they require in order to perform their work and tasks;
- users may not have access to applications and data for which they were not assigned any access rights;
- users may not have access to data/information that is classified with a level of confidentiality for which they have no authorisation.

Access to applications and data that the user does not need to perform their work and tasks shall not be permissible even if such access is not restricted for the user.
Users shall be responsible for all activities performed with their user identification and password or their qualified digital certificate.

Article 17
(System passwords)

(1) All systems' passwords and procedures used for access and administration within the PC network, email administration and administration via application software shall be stored in sealed envelopes in fireproof cabinets or safes at the UL Rectorate or a member faculty's Dean's Office if this is a system that is not part of the UL system.
(2) Protected passwords stored in sealed envelopes may be used in exceptional and emergency circumstances. Every instance of using the content of sealed envelopes shall be documented.
(3) After using passwords from the sealed envelopes, the Secretary General or a member faculty's secretary shall determine new passwords at the proposal of the UL IT Department.

Article 18
(Backup copies)

(1) For the purposes of restoring personal data or a computer system following a breakdown or loss of data for other reasons, an appropriate service or worker, appointed for the UL by the Secretary General and by a member faculty's secretary for said member faculty, shall make copies of personal data filing systems on a regular basis and shall appropriately document the making of such copies.
(2) The copies referred to in the preceding paragraph shall be stored in places dedicated for this purpose, which must be fireproof, flood-proof, secure from electromagnetic disturbances, within the framework of the prescribed climatic conditions, and which shall be locked by anti-theft means. These places shall be physically separate from the location of the UL or a member faculty, and the physical transfer between the two locations may only be carried out by an authorised person appointed for the UL by the Secretary General and for a member faculty the secretary of said member faculty. At no point in the physical transfer may such a copy be left unsupervised.

Article 19
(Safeguarding of archives)

(1) The premises containing archive materials which contain personal data shall meet the applicable internationally recognised standards of safeguarding archive materials.
(2) Regardless of the preceding paragraph, the premises containing archive materials with personal data carriers (including physical documents) shall be at least fireproof and theft-proof, as well as physically appropriate in a way that prevents the destruction of personal data due to floods, water spillage or other accidents and environmental impacts.

Chapter IV
SERVICES PROVIDED BY EXTERNAL LEGAL ENTITIES OR NATURAL PERSONS

Article 20
(Obligation to sign a personal data processing contract)

(1) Every external legal entity or natural person that performs tasks relating to the processing (i.e., including consultation) of personal data (the processor) and has at least the option of accessing personal data, shall sign a written contract on the processing of personal data. Such contracts shall also prescribe the conditions and measures for ensuring safe personal data processing or the processor shall be bound to adhere to these Rules. This shall also apply to external entities that maintain hardware and software and that produce and install new hardware or software.
(2) External legal entities and natural persons may provide personal data processing services only pursuant to the client's authorisations, and may not process or otherwise use data for any other purpose.
(3) An authorised legal entity or natural person that performs the agreed services for the University of Ljubljana or its member faculty outside the controller's premises shall operate a personal data protection regime that is at least as strict as that set out in these Rules.

Chapter V
RECEIPT AND TRANSMISSION OF PERSONAL DATA

Article 21

(Incoming mail)

(1) The employee in charge of receiving and recording postal items shall deliver a postal item containing personal data directly to the individual or service to which the item is addressed.
(2) The employee in charge of receiving and recording postal items shall open and inspect all postal items and items arriving to the UL Governing Board or member faculty in some other way (brought in by customers or couriers, except for items referred to in the third and fourth paragraphs of this article).
(3) The employee in charge of receiving and recording postal items shall not open items addressed to another body or organisation, items that have been delivered in error or items marked as containing personal data or items that are marked on the envelope as relating to a competition/tender. If a postal item is addressed to another body or organisation and has been delivered to the UL or a member faculty in error, the employee in charge of receiving and recording postal items shall promptly send it to the addressed body or organisation, with *mutatis mutandis* application of the provisions of the act governing the general administrative procedure.
(4) The employee in charge of receiving and recording postal items shall not open items addressed to an employee, where it is stated on the envelope that it should be delivered personally to the addressee, and items where the name of the employee is stated first, without an indication of their official position, and is only then followed by the UL's or member faculty's address.

Article 22
(Transmission of personal data)

(1) Personal data may only be transferred using information, telecommunication and other resources if procedures and measures have been put in place to prevent unauthorised persons from processing it or learning of its content without authorisation.
(2) Personal data in physical form shall be sent by registered post.
(3) An envelope in which personal data is sent shall be such that the content of the envelope is not visible under normal lighting conditions or made visible when the envelope is illuminated using normal lighting. The envelope shall also be such that it cannot be opened or its content viewed without visible traces of such actions being left.
(4) Special categories of personal data (formerly known as sensitive personal data) in physical form shall be sent to addressees in sealed envelopes via a courier or with proof of delivery. Such data shall be specially marked and protected during processing in order to prevent unauthorised persons from having access to it.
(5) Special categories of personal data in electronic form may be transmitted via telecommunications networks only if specially secured by cryptographic methods and an electronic signature so that data cannot be read during transmission.

Article 23
(Conduct upon transmission of personal data)

(1) Personal data shall only be sent to those users who can demonstrate an adequate legal basis or produce a written request, or with the consent of the data subject.
(2) The external user shall file a written request for every transmission of personal data containing a clear reference to the legal provision authorising the user to obtain personal data, or shall enclose with the application a written request or the consent of the data subject.
(3) Each and every time that personal data is sent it is noted in the record of items sent, which must clearly show which personal data was supplied, to whom, when and on what legal basis.
(4) Original documents may not be transmitted unless by written order of a court. For periods when no original document is available, a copy shall be provided instead.
(5) Reviewing and copying administrative files and providing notices on the course of the procedure shall be carried out in accordance with the provisions of the act governing the general administrative procedure.

Chapter VI
DELETION OF DATA

Article 24
(Deletion method)

(1) After the expiry of the storage period/purpose, personal data shall be deleted, or data carriers shall be irreversibly destroyed.
(2) Deletion of personal data on computer media shall be done in such a way following a procedure and a method that makes it impossible to restore deleted data.
(3) Personal data contained in the traditional data carriers (documents, files, registers, lists) shall be deleted by destroying the carriers. The carriers shall be destroyed physically (burned, cut) on the institution's premises or under the supervision of the institution's authorised employee at an organisation whose business is disposal of confidential documents.
(4) Destruction and deletion of personal data shall be done on a commission basis. The Secretary General or a member faculty's secretary shall appoint a three-member commission with a permanent mandate, which shall be present and make a report on every deletion and destruction of personal data carriers.

Article 25

(Deletion of ancillary documentation)

(1) Ancillary documentation, drafts, computer products or semi-finished products and templates that contain individual pieces of personal data shall also be deleted and destroyed with all the diligence and care set forth in these Rules.
(2) The destruction of personal data on carriers referred to in the previous paragraph shall be carried out regularly and promptly.

Chapter VII
MEASURES TAKEN IN RESPONSE TO ABUSE OF PERSONAL DATA OR A PERSONAL DATABASE BREACH

Article 26
(Obligation to inform about and prevent further damage)

(1) The employees are required to inform the UL DPO and/or appropriate UL or member faculty's service as determined by the Secretary General (for the UL) or a member faculty's secretary (for said member faculty) of any activities related to the disclosure or unauthorised processing of personal data, malicious or unauthorised use, appropriation, modification or damage of data immediately after detecting any incident or loss event, and shall themselves try to prevent such activity. The employees shall not risk their life or health in doing so.

Article 27
(Notifying the Information Commissioner)

(1) In the event of a personal data breach, the Rectorate shall consult with the UL DPO, and the Dean's Office shall consult with the member faculty's DPO, before notifying the Information Commissioner. The Rectorate/Dean's Office shall notify the Information Commissioner of the Republic of Slovenia about the breach no later than within 72 hours after learning about the breach, unless there is no likelihood that the rights and freedoms of data subjects would be infringed upon through the personal data breach. To notify the Information Commissioner, the latest published form of the Information Commissioner of the Republic of Slovenia shall be used or, alternatively, the form prescribed by the UL DPO.
(2) The notice referred to in the preceding paragraph shall contain the following information:
• a description of the type of personal data breach, the categories and approximate number of data subjects concerned, and the types and approximate number of personal data records concerned;
• notification about the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
• a description of the likely consequences of the personal data breach;
• a description of the measures taken or proposed to be taken by the UL or a member faculty to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
(3) If the information referred to in the previous paragraph cannot be communicated in full, it shall be communicated gradually, i.e., immediately once it becomes known.
(4) If a personal data breach took place at the processor, the latter shall inform the controller no later than within 24 hours. Such a provision shall be included in every contract on contractual processing, which the UL or a member faculty enters into with the processor.
(5) The person investigating the incident/eliminating any consequences of the incident shall document every personal data breach, including the facts in connection with the personal data breach, the effects of the breach, and the remedial actions taken. The UL or the member faculty shall disclose this documentation to the Information Commissioner of the Republic of Slovenia if the latter requires it to do so.

Article 28
(Notifying the data subject)

(1) If the UL DPO or a member faculty's DPO estimates it likely that the personal data breach has caused a high risk to the rights and freedoms of data subjects, the Rectorate or the Dean's Office shall notify the data subject that a personal data breach has taken place no later than within 24 hours.
(2) The notification referred to in the preceding paragraph shall be written in clear and simple language and shall contain the following:
• notification about the name and contact details of the UL's or member faculty's Data Protection Officer or other contact point where more information can be obtained;
• a description of the likely consequences of the personal data breach;
• a description of the measures taken or proposed to be taken by the UL or a member faculty to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
(3) A notification need not be sent to the data subject referred to in the first paragraph in the following cases:
• the competent service at the UL or member faculty has taken appropriate technical and organisational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
• the competent service at the UL or member faculty has taken subsequent measures to ensure that the high risk to the rights and freedoms of data subjects referred to in the first paragraph will probably no longer occur;

• in cases where such notification would require disproportionate effort. Therefore, in such a case, there shall be a public communication or a similar measure, whereby the data subjects are informed in an equally effective manner.

Chapter VIII
RESPONSIBILITY FOR IMPLEMENTING PERSONAL DATA PROTECTION MEASURES

Article 29
(Signing a statement of familiarity with the Rules)

1. Before a worker commences work or begins collaborating with the UL or a member faculty in any other way, the worker/contractor (including a student performing student work, or members of the UL bodies or working bodies of the UL Senate) shall be familiarised with these Rules, whereon a statement of familiarity is usually signed. The obligation of adhering to these Rules shall also be applicable if an individual refuses to sign the statement. The Rectorate's/member faculty's professional associate shall make a note of the refusal to sign the statement.
2. The obligation to safeguard personal data shall apply permanently, even after the end of employment/collaboration.

Article 30
(Conduct in the event of suspecting an administrative or criminal offence)

(1) If an administrative offence is suspected in a specific case, the Rectorate or the Dean's Office shall notify the Information Commissioner of the Republic of Slovenia.
(2) If a criminal offence is suspected in a specific case, the Secretary General or a member faculty's secretary shall inform the Police and the competent prosecuting authority.

Chapter IX
KEEPING OF RECORDS

Article 31
(Record of processing activities)

(1) The UL and member faculties shall keep a Record of Personal Data Processing Activities in line with the provision under Article 30 of the Regulation. The Record shall be updated regularly, with a mandatory update once a year.

Chapter X
SPECIAL ARRANGEMENTS
Article 32
(Special arrangement for specific activities)

(1) These Rules shall apply to the UL and all member faculties within the entire scope of their operations.(2) If a member faculty, its DPO or the UL DPO estimates that a member faculty should arrange the processing security in a certain part of its operations or performance of tasks in greater detail than set forth by these Rules, the member faculty may do so, provided that the special arrangement achieves at least the same standards of security as stipulated in these Rules. Before adopting special rules, consent from the UL DPO shall be obtained.

Chapter XI TRANSITIONAL AND FINAL PROVISIONS

Article 33
(Alignment of the records of processing activities)

(1) The UL and member faculties shall, within 3 months of adopting these Rules, appoint persons responsible for individual filing systems of personal data or processing processes in their records of processing activities.
(2) For each position that may, due to the nature of its work, process personal data, the UL and member faculties shall, within 3 months of adopting these Rules, determine access rights for both physical and electronic forms of filing systems or processes.

Article 34
(Alignment of personal data processing contracts)

(1) The UL and member faculties shall, within 3 months of adopting these Rules, align personal data processing contracts, statements, records of processing activities and any other documents governed by these Rules.
(2) All personal data processing contracts concluded before 25 May 2018 shall be replaced by the UL and member faculties with processing contracts that contain all the components as determined by Article 28 of the Regulation.

Article 35

Within 1 month of publishing these Rules, the UL and member faculties shall notify all employees and external contractors performing personal data processing activities of this (including students performing work based on a referral from the student employment service).

Article 36

(1) These Rules shall enter into force on the 15th day after being posted on the University of Ljubljana website.
(2) Rules on the Protection of Personal and Confidential Data at the University of Ljubljana dated 9 October 2006 shall cease to be in force.
(3) These Rules shall be published on the intranet and the message board (where applicable) of the UL and all member faculties.

Ljubljana, 2 April 2020

Governing Board of the University of Ljubljana:
Prof. Borut Božič, President

APPENDICES:

Appendix 1

Statement by a worker/contractor on personal data security

The undersigned _____ hereby confirm that I have read the Rules on the Secure Processing of Personal Data at the University of Ljubljana, that I understand them and undertake to explicitly enforce them throughout my time working for the University of Ljubljana or the faculty, as well as after I complete my work.

I also confirm that I am familiar with the provisions of the act governing personal data protection, and the General Data Protection Regulation (GDPR), and with the consequences of any failure to adhere to the aforementioned Rules, act or Regulation (breach of employment contract). I am also familiar with the fact that I will be regressively responsible if the University of Ljubljana or the faculty at which I am employed has to pay a fine, penalty or damages due to unlawful interference with the personal data protection caused intentionally or due to gross negligence through my conduct.

Signature: _____ Date and place: _____

Appendix 11

Statement by an external provider on personal data security

I, the undersigned _____, hereby confirm that I have read the Rules on the Secure Processing of Personal Data at the University of Ljubljana, that I understand them and undertake to explicitly enforce them throughout my time working for the University of Ljubljana or the faculty, as well as after I complete my work.

I also confirm that I am familiar with the provisions of the act governing personal data protection, and the General Data Protection Regulation (GDPR), and with the consequences of any failure to adhere to the aforementioned Rules, act or Regulation (breach of contract). I am also familiar with the fact that I will be held liable if the University of Ljubljana or the faculty at which I am employed has to pay a fine, penalty or damages due to unlawful interference with the personal data protection caused intentionally or due to gross negligence through my conduct.

Signature: _____ Date and place: _____

Appendix 12

SAMPLES OF PERSONAL DATA TRANSMISSION

Title of the member faculty/university, address

_____
_____
_____

Ljubljana, _____

Ref. No.: _____

1. **A RECORD OF INSTANCES OF REMOVAL OF A PERSONAL DATA CARRIER FROM THE PREMISES**

Date of removal	Reason	Authorisation	Date of return	NOTES

2. **RECORD OF TRANSMITTING PERSONAL DATA TO THIRD PARTIES (optional in the event of another form of traceability)**

Date of transmission	Reason (legal basis)	Authorisation	NOTES

3. **RECORD OF COPIES MADE OF THE CONTENT OF PERSONAL DATA FILING SYSTEMS (optional in the event of another form of traceability)**

Date of creating copies	Type of filing system copied	Purpose for which copies were used	Copy storage location	Copy destruction date	NOTES

4. RECORD OF EXERCISING DATA SUBJECTS RIGHTS (optional)

Date of request	Type of right	Decision	Date of decision	NOTES

5. RECORD OF MODIFICATIONS AND UPDATES TO SYSTEM AND APPLICATION SOFTWARE

Date of intervention in the software	Type of intervention	Name and surname of the person who performed the intervention	Purpose of intervention	Signature of person	NOTES

Appendix 14

List of security policies of the UL/member faculty relating to the personal data processing security/information safeguarding:

a. (security policy)
b. (security policy)
c. ...