Based on point 4 of Article 253 of the University of Ljubljana Statutes (Official Gazette of the Republic of Slovenia, No. 8/2005), Articles 24 and 25 of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 86/04) and Articles 83 and 84 of the Higher Education Act (Official Gazette of the Republic of Slovenia, No. 100/2004 – official consolidated text) and following a discussion at the session of the Governing Board of the University of Ljubljana dated 28 September 2006, the Secretary General of the University of Ljubljana laid down on 2 October 2006 the following

RULES
on the protection of personal and confidential data at the University of Ljubljana

I. GENERAL PROVISIONS

Article 1

These Rules establish the organisational, technical and logistically technical procedures and measures to protect personal data at the University of Ljubljana and its Member Faculties in order to prevent any accidental or intentional unauthorised destruction of data, their change or loss and any unauthorised access, processing, use or disclosure of personal data.

Employees and external associates (technical associates and members of University and Member Faculty bodies) who process and use personal data in their work must have knowledge of the Personal Data Protection Act, the legislation governing the areas of their work and of the contents of these Rules.

Article 2

The expressions used in these Rules shall have the following meanings:

1. ZVOP-1 – Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 86/2004 and 113/05);
2. Personal data – shall be any data relating to an individual, irrespective of the form in which it is expressed;
3. Individual – shall be an identified or identifiable natural person to whom the personal data refers; a natural person is identifiable if he/she can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity, whereby the method of identification does not incur major costs or require considerable time;
4. Personal data collection – shall mean the aggregation of any structured set of personal data that is accessible based on the criteria providing the use or further aggregation of data, irrespective of whether the set is centralised, decentralised or dispersed on a functional or geographic basis; a structured set of data shall mean a data set that is organised in a manner identifying or providing the identifiability of an individual;
5. Personal data processing – shall mean any operation or set of operations which is performed in relation to the personal data processed by automatic means or part of or intended to be included in a personal data collection when processed manually, in particular collection, acquisition, entry, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, communication, dissemination or otherwise making available, classification or integration, blocking, anonymisation, deletion or destruction; processing can be manual or automated (means of processing);
6. Personal data controller – shall mean a natural person or legal entity or some other public or private sector entity which alone or jointly with others determines the purposes and means of processing personal data, or an entity set forth by an act also specifying the purposes and means of processing;
7. Sensitive personal data – shall mean data revealing the racial, national or ethnic origin, political, religious and philosophical beliefs, trade-union membership, health condition, sex life, entry to or deletion from criminal or offence records and biometric features;
8. Personal data user – shall be a natural person or legal entity or some other public or private sector entity to which personal data is transmitted or disclosed;

9. Data medium – shall be any type of medium on which data (documents, acts, materials, briefs, computer equipment including magnetic, optical or other computer media, photocopies, audio and visual material, microfilm, data transfer devices, etc.) is written or recorded;

Protected personal data shall be deemed to be data about a natural person revealing the features, situations or relationships of an individual, irrespective of the form in which they are expressed.

In terms of the provision of paragraph 1 of this Article, personal data about a natural person shall, in particular, be deemed to be:

- identification data about an individual,
- data referring to racial origin and affiliation to a nation or nationality,
- data referring to family relationships,
- data referring to housing and dwelling conditions of an individual,
- employment data,
- data revealing the social and economic situation of an individual,
- data revealing the education and skills acquired,
- data on the use of communication means,
- data on spare-time activities,
- data on an individual's health condition,
- data on ideological and religious beliefs,
- data on an individual relating to internal matters,
- data on an individual's habits.

Article 3

Personal data protection shall cover the legal, organisational and relevant logistical and technical procedures and measures taken to:

- secure the premises, equipment and system software;
- secure the application software used to process personal data;
- provide the security of transmission and transfer of personal data;
- prevent unauthorised persons from accessing the devices used to process personal data and their collections.

Article 4

The processing and protection of sensitive personal data including data revealing the racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health condition, sex life, entry to or deletion from criminal or offence records and biometric features shall be carried out with due care and diligence.

Sensitive personal data shall be specially labelled (CONFIDENTIAL) and protected during processing, so as to prevent unauthorised persons from accessing them.

II. SECURITY OF PREMISES AND COMPUTER EQUIPMENT

Article 5

The premises containing the media carrying protected personal data – every document that includes personal data and any other computer or electronic data medium – as well as hardware and software (hereinafter "secured premises") shall be protected by organisational, physical and technical measures to prevent unauthorised persons from accessing the data.

Access to the secured premises indicated in paragraph 1 of this Article shall only be possible and allowed during working hours, while access outside working hours shall only be allowed based on an authorisation by the Secretary General at the Administration and the Secretary of a Member Faculty at a faculty.

Personal data media that are stored outside active work premises or outside secured premises (hallways, common premises, active and passive archives, etc.) are to be locked at all times in a fire-resistant protected cabinet.

Keys to the secured premises shall be kept in the premises specified by the house rules of the University of Ljubljana Administration and the house rules of Member Faculties, while unusable keys are to be destroyed before a commission. For example, keys shall not be left in the door lock on the exterior side.

Secured premises shall never remain unsupervised or, rather, shall be locked upon absence of employees supervising them.

Article 6

Outside working hours, personal data media are to be kept in locked fire-resistant cabinets in working premises.

Computers or other hardware used to process or store personal data shall be turned off and locked physically or by software outside working hours, and access to the personal data stored on the computer disk shall be encoded.

Computers that must be connected at all times due to permanent access are to be protected in terms of paragraph 1 of Article 5.

Article 7

Persons who are not employees shall not be allowed to enter the secured premises (secretariat, HR office, counselling office, payroll office, passive archives, etc.) unescorted or without the presence of an employee. An employee working in the secured premises is required to supervise the premise with due care and diligence and to lock it upon leaving it.

An employee who uses or processes personal data in any way during their work shall not leave personal data media on a desk during working hours or leave them in any other way exposed to the risk of consultation by unauthorised persons or employees.

Data media and computer displays in premises accessible to customers or persons not employed at the establishment are to be installed so as to prevent them from consulting them during processing or working with them.

Article 8

Employees are not allowed to take personal data media out of the establishment without the express authorisation of the University Secretary General or a Member Faculty Secretary relating to the data kept at a Member Faculty.

The processing of personal data from personal data collections shall only be permitted in the premises of the establishment.

The Secretary General of the University or the Secretary of a Member Faculty may permit that personal data media be taken out of the establishment only on the condition that an employee has entered in advance the purpose and reason for taking data out of the establishment in the record of personal data handling.

Any disclosure of personal data to authorised external institutions and others proving the legal basis for the acquisition of personal data shall be authorised by the Secretary General of the University.

Any forwarding of personal data from the previous paragraph of this Article shall be entered in the record of personal data handling.

Article 9

The maintenance and repair of hardware and other equipment used to process personal data shall only be allowed with the knowledge and approval of the Secretary General of the University or the Secretary of a Member Faculty or a person authorised by them, and shall only be carried out by authorised repair services and their maintenance officers who have concluded a software and hardware service contract with the establishment.

Article 10

Persons maintaining premises and other equipment in the secured premises, business partners and other visitors may move in the secured premises only upon the presence of an employee.

Article 11

Employed technical maintenance officers and cleaning staff may move in the secured premises outside working hours and without the presence of a responsible officer only if data media are stored in locked cabinets in the manner laid down by these Rules for the time outside working hours.

III. PROTECTION OF SYSTEM AND APPLICATION SOFTWARE AND COMPUTER-PROCESSED DATA

Article 12

Access to software is to be protected in a manner allowing access only to specified authorised employees and officers contracted by the establishment to service the hardware and software.

Article 13

Any repairs, alterations and updates to the system and application software shall only be allowed based on an approval by the Secretary General or the Secretary of a Faculty Member or a person authorised by them and may only be carried out by an authorised service and organisation or its employees who have concluded a relevant contract with the establishment.

Operators are required to properly document the alterations and updates to the system and application software.

Article 14

The storage and protection of application software shall be subject to the same provisions as for other data deriving from these Rules.

An employee must be authorised to process and handle personal data on a computer to ensure that any copy of personal data made upon servicing, repairs, alterations or updates to the system or application software be destroyed after the need for it has expired.

An employee who is authorised to process and handle personal data on a computer shall attend and supervise the servicing of hardware and software at all times in order to prevent any unlawful handling of personal data.

If it is required to repair a computer containing a disk with personal data outside the establishment and without the supervision of an authorised employee, the data are to be deleted from the disk in a manner preventing their restoration. If such deletion is not possible, the repair shall be made in the business premises of the establishment in the presence of an authorised employee.

Article 15

The content of network server disks and local workstations where personal data are stored shall be scanned for computer viruses pursuant to the scanning plan.

Upon the occurrence of a computer virus, it is required to do everything to eliminate the virus with the help of experts and identify the cause of the virus.

All data and software intended to be used on University computers and in the University computer information system and which arrive at the establishment on computer data transmission media or via telecommunication channels are to be scanned for the presence of computer viruses prior to their use.

Article 16

Employees are not allowed to install software without the express authorisation of the Secretary General or the Secretary of a Member Faculty.

Employees are not allowed to take software out of the establishment without the express authorisation of the Secretary General or the Secretary of a Member Faculty.

Article 17

Access to data via application software is to be protected with a system of passwords for the authorisation and identification of software and data users. The Secretary General shall define the regime of assigning, storing and changing passwords at the proposal of the University ICT Office.

Article 18

All passwords and procedures used for access and administration in a PC network, administration of email and administration via application programs shall be kept in sealed envelopes and protected in a fire-resistant cabinet at the establishment.

The secured passwords kept in sealed envelopes may only be used in extreme and urgent cases. Each use of the content of the sealed envelopes shall be documented.

After passwords from sealed envelopes are used, the Secretary General or the Secretary of a Member Faculty shall set new passwords at the proposal of the University ICT Office.

Article 19

To restore personal data or a computer system following a malfunction or loss of data for other reasons, the employee keeping the personal data collections is required to make copies of the contents of the personal data collections kept by them on a regular basis.

Computer copies of the contents of personal data collections on floppy discs, compact discs or other media shall be kept in secured and locked cabinets that are fire-resistant, flood-resistant and resistant to electromagnetic interference and under the prescribed ambient conditions.

IV. SERVICES RENDERED FOR EXTERNAL LEGAL ENTITIES OR NATURAL PERSONS

Article 20

A written contract as foreseen in paragraph 2 of Article 11 of the Personal Data Protection Act shall be concluded with each external legal entity or natural person performing individual tasks related to the collection, processing, storage or disclosure of personal data and who is registered to pursue such activities (contract processor). Such contract is to stipulate the conditions and measures to ensure personal data protection and their security. This paragraph also applies to outside persons maintaining hardware and software and producing and installing new hardware or software.

External legal entities or natural persons may perform only the services of personal data processing within the scope of the client's authorisations and cannot process or use data in any other way or for any other purpose.

An authorised legal entity or natural person rendering the agreed services for the University of Ljubljana or its Faculty Member outside the manager's premises is to have an equally strict method of personal data protection to that foreseen in these Rules.

V. RECEPTION AND DISCLOSURE OF PERSONAL DATA

Article 21

An employee in charge of receiving and recording mail is to hand over a postal item with personal data directly to the individual or service it is addressed to.

An employee in charge of receiving and recording mail shall open and review all postal items and parcels that arrive in some other way at the University of Ljubljana Administration or a Member Faculty (are brought by customers or couriers, except for the parcels set forth in paragraphs 3 and 4 of this Article).

An employee in charge of receiving and recording mail shall not open the parcels addressed to some other body or organisation and delivered by mistake, and the parcels labelled as personal data or with an indication on the envelope from which it derives that they refer to a competition or invitation to tender.

The employee in charge of receiving and recording mail shall not open any parcels addressed to an employee if it is stated on the envelope that they are to be delivered in person to the addressee, nor parcels on which the name of an employee, without his or her official rank, is indicated first and the University or Faculty Member address indicated second.

Article 22

Personal data may be transmitted by information, telecommunication and other means solely under the implementation of procedures and measures that prevent unauthorised persons from taking possession of or destroying data and unlawfully learning their content.

SENSITIVE PERSONAL DATA shall be sent to addressees in sealed envelopes and require a signature in the delivery book or with proof of service.

Personal data shall be sent by registered mail.

The envelope in which personal data is sent is to be made in a way preventing the visibility of its contents when exposed to normal or artificial light. Furthermore, the envelope must be such that it cannot be opened and its contents examined without a visible trace.

Article 23

The processing of sensitive personal data is to be specially labelled and secured.

The data from the previous paragraph may be transmitted via telecommunication networks only if they are protected by cryptographic methods and electronic signature, so as to ensure that data are unreadable during transfer.

Article 24

Personal data shall only be disclosed to users who demonstrate a suitable legal basis or a written request or consent of the individual to whom the data refers.

Any disclosure of personal data shall be subject to the submission of a written application by the person entitled and clearly indicating the provision of the act empowering the applicant to obtain personal data, or shall have attached to the application a written request or consent of the individual to whom the data refers.

Any disclosure of personal data shall be recorded in disclosure records revealing which personal data was disclosed to whom, when and on what grounds (Article 22 of the Personal Data Protection Act).

No original documents shall be disclosed unless so ordered in writing by the court. During the term of absence, an original document is to be replaced by a copy.

Article 25

Any examination and copying of administrative files and notifications on the course of proceedings shall be made in line with the provisions of Article 82 of the General Administrative Procedure Act.

Examination and copying of administrative files shall only be allowed to clients in proceedings and to persons proving their legal benefits in their written applications, i.e. in the presence of an officer. Before examining or copying an administrative file, it is required to check the identity of the client or the person entitled by examining their identity card, passport or driver's licence.

During each examination or copying of data from an administrative file, an official note is made which is entered in the file. The official note, which must also be signed by the person entitled, is to clearly show the number of the file, the date and time of examination, the name and address of the person entitled, and the number and type of document showing the identity and purpose for which the examination or copy was made. If an administrative file also contains personal data, the person liable is to be warned of the obligation to protect such data, which must also be evident from the official note.

VI. DELETION OF DATA

Article 26

Personal data can only be kept in a personal data collection for the term required to achieve the purpose for which they are collected and kept.

After the need for personal data management has expired, the data shall be deleted or data media destroyed.

Article 27

Deletion of personal data on computer media is to be made in a manner, procedure and method preventing the restoration of the data deleted.

The personal data contained on classic media (documents, files, register, list) are to be deleted by destroying the media. The media are to be physically destroyed (burned, cut) in the premises of the establishment or under the supervision of an employee authorised by the establishment in the premises of an organisation dealing with the destruction of confidential documents.

The destruction and deletion of personal data is to be performed before a commission. The Secretary General or the Secretary of a Member Faculty shall appoint a 3-member commission with a permanent term of office to attend and make an official record of each deletion and destruction of personal data media.

Article 28

Supporting documents or computer products or templates containing individual personal data are to be deleted and destroyed with all due care and diligence as set forth in these Rules.

The destruction of personal data on the media from the previous paragraph is to be carried out promptly and regularly.

VI. ACTIONS TO BE TAKEN UPON THE DISCOVERY OF PERSONAL DATA ABUSE OR INTRUSION IN A PERSONAL DATA COLLECTION

Article 29

University employees shall be obliged to implement measures to prevent any abuse of personal data and shall handle the personal data encountered during their work with due care and diligence in the manner of and following the procedures set forth by these Rules.

An employee who learns or notices an abuse of personal data (detection of personal data, unauthorised destruction, unauthorised changes, damage to the collection, appropriation of personal data) or an intrusion in a personal data collection is required to immediately inform the Secretary General of the University or the Secretary of a Member Faculty and the person authorised to keep and edit the personal data collection which was abused or breached.

Article 30

The Secretary General or the Secretary of a Member Faculty is required to take appropriate actions against a person abusing personal data and breaking into a personal data collection without authorisation.

If there is any suspicion that an intrusion in a personal data collection has been committed with the intent and purpose to abuse personal data or use them contrary to the purposes for which they were collected, or if the abuse of personal data has already taken place, the Secretary General or the Secretary of a Member Faculty is required to report the intrusion or abuse or the attempt to abuse to law enforcement authorities in addition to introducing a disciplinary proceeding against the perpetrator, pronouncing a reprimand preceding regular termination of the employment contract, regular termination of the employment contract for reasons of fault or extraordinary termination of the employment contract if the abuse or attempted abuse was committed by a University employee.

A personal data abuse shall be deemed to be any use of personal data for the purposes not compliant with the purposes of collection as laid down by the act providing the basis for their collection or the purposes specified in the register of personal data collections. An attempt to abuse shall be deemed to be any attempt to abuse personal data for illicit purposes.

VII. RESPONSIBILITY FOR THE IMPLEMENTATION OF MEASURES TO PROTECT PERSONAL DATA

Article 31

Before an employee takes up work at a post where personal data or personal data media are collected, edited, processed, changed, stored, disclosed or used, the employee is required to sign a statement obliging them to protect personal data as professional secrecy and warning them of the consequences of violating the commitment (an Article in the employment contract or a declaration in case of casual labour).

Before taking up a function (membership) in a University or Member Faculty body dealing with personal data of employees and students, the member of such body is to sign a declaration obliging them to protect personal data and warning them of the consequences of violating the commitment.

The obligation to protect the personal data encountered by an employee during their work shall continue to apply after the employment relationship at the establishment is terminated.

Article 32

An employee shall commit a violation of their duties:

- if they omit conscientious and due supervision of the secured premises;
- if they omit actions to prevent access to data or personal data media;
- if they fail to destroy a copy of personal data in cases set forth in paragraph 2 of Article 14;
- if they are not present throughout the servicing of hardware and software;
- if they fail to carry out prevention relating to computer viruses;
- if they fail to keep a record of the copies of personal data collection contents in the record of personal data handling;
- if they fail to inform the Secretary General or authorised employee of an abuse of personal data or an intrusion in a personal data collection.

Article 33

An employee shall commit a serious violation of their duties:

- if they communicate the personal data encountered during their work to colleagues or other persons;
- if they omit the care and supervision over personal data media during working hours, thereby allowing unauthorised persons the possibility of consulting them;
- if they make unauthorised copies of personal data media;
- if they take personal data media out of the establishment without an explicit authorisation;
- if they disclose personal data to authorised external institutions without the authorisation of the Secretary General, the Secretary of a Member Faculty or a person authorised by them;

- if they fail to enter the disclosure of personal data to external institutions in the record of personal data handling;
- if they repair, alter or update system or application software;
- if they install or take software out of the establishment without the explicit authorisation of the Secretary General, the Secretary of a Member Faculty or a person authorised by them;
- if they fail to make copies of personal data on a regular basis;
- if they fail to store computer copies of personal data collection contents in secured locked cabinets.

Article 34

Any abuse or suspected abuse of the personal data kept in the University personal data collections by persons who are not University employees shall be reported to law enforcement authorities.

VIII. SPECIAL REGULATIONS FOR THE PERSONAL DATA COLLECTIONS KEPT AT THE ESTABLISHMENT

1. Responsible employees

Article 35

The set-up, management, updating and handling of the personal data collections and personal data kept at the establishment shall fall within the responsibility of the Secretary General at the University, Secretaries at Member Faculties or persons authorised by them in writing.

2. Authorised employees

Article 36

The Rector, Vice-Rectors, Secretary General and his/her assistant at University level may consult and use the personal data contained in all personal data collections kept at the University for the purposes of their work. Member Faculty Deans, Vice Deans and Secretaries shall be authorised to consult and use the personal data contained in all personal data collections kept at a Faculty Member for the purposes of their work.

3. Personal data collections requiring consent

Article 37

To set up and keep personal data collections referring to the study process and having no legal basis in acts, the establishment must obtain the written consent of the relevant student. This shall be done by providing students with a statement on the enrolment form to be signed upon enrolment and allowing the use of the personal data entered in the enrolment form for the purposes of libraries, admission procedures for student dorms, etc.
The establishment is also required to obtain the written consent of employees or persons to whom personal data refer in order to set up a personal data collection or maintain personal data that the establishment intends to keep and for which such database or personal data collection is not laid down by the law.

Article 38

The written consent from the previous Article shall contain:
- clearly defined will for the issue of the consent;
- an indication of the data to be collected;
- a precisely defined purpose of data collection;
- assurance that the data will only be used for the purpose for which they have been collected;
- the period of data storage;
- an indication of the possibility of cancelling the consent;
- the date of signing the statement and the person's signature.

4.Keeping and updating personal data collections

Article 39

The personal data collections of students shall be set up and updated upon enrolment in the establishment and at the beginning of each academic year.

The data in personal data collections of students are set up and updated by the authorised employees of the Dean's Office.

Article 40

5. Storage and storage periods of personal data collections

The storage of personal data collections shall fall under the responsibility of employees who are authorised to process personal data collections.

Enrolment forms containing data about the students enrolled in the establishment shall be kept at Member Faculties in a locked fire-resistant cabinet and the keys to them may only be given to authorised employees. The data storage period is indicated in the register of collections.

Article 41

The personal data collections of employees, i.e. HR records, shall be kept in a locked fire-resistant cabinet at the Secretariat and Accounting Office of a Member Faculty and the University HR Management Office (the precise definition of the storage of collections is indicated in the register of personal data collections).

Article 42

Storage periods for personal data collections shall be specified for each personal data collection in the register of personal data collections.

Personal data collection registers, grouped in the Internal list of personal data collection registers, shall form an annex to these Rules.

IX. TRANSITIONAL AND FINAL PROVISIONS

Article 43

The Internal list of collection registers and personal data collections, the organisation of personal data protection and other matters set forth by these Rules are to be harmonised with the Personal Data Protection Act and the provisions of these Rules within 60 days of the adoption of these Rules.

Article 44

These Rules shall be laid down by the Secretary General of the University following a discussion at a session held by the University of Ljubljana Governing Board.

Amendments and supplements to these Rules shall be laid down by the Secretary General of the University under the same procedure.

Article 45

All University employees are required to be acquainted with the provisions of these Rules.

These Rules shall be received by the services or employees with a job duty to collect, edit, process, change, store, disclose or use personal data or personal data media.

Article 46

Employees on posts involving the collection, editing, processing, changing, storage, transmission or use of personal data or personal data media are required to sign a statement as per Article 31 hereunder within 30 days of the adoption of these Rules (the sample statement forms an annex to these Rules).

Members of University and Member Faculty bodies are required to sign the statement referred to in Article 31 of these Rules at the constituent meeting of the relevant body.

Article 47

These Rules shall enter into force and become applicable on the 8th day following their publication on the University of Ljubljana website.

These Rules were considered by the University of Ljubljana Governing Board at its session held on 28 September 2006, and laid down by the Secretary General on 2 October 2006.

These Rules were published on the University of Ljubljana website on 9 October 2006.

Ljubljana, 9 October 2006

Secretary General of the University of Ljubljana

(Mihaela Kranjc, LLB)

ANNEXES:

Sample form 1

EMPLOYEE'S STATEMENT ON PERSONAL DATA PROTECTION

Name of Faculty Member/University

Address

_____

_____

_____

Ljubljana, _____

No.: _____

I, the undersigned,_____, born on_____, residing at _____

_____, employed at the post _____,

aware of the nature of personal data that I will collect, edit, process, change, store, disclose or use in my work as an employee of the University of Ljubljana (Member Faculty), hereby

D E C L A R E

to safeguard all personal data encountered during my work as professional and business secrecy.

I, the undersigned, have been instructed and am aware that the disclosure of the personal data encountered during my work to unauthorised persons or the abuse of such data is sanctioned as a serious breach of working obligations and as a criminal offence and is, at the same time, a reason for the termination of the employment contract for reasons of fault.

Employee's signature:

_____

Sample form 2

STATEMENT ON PERSONAL DATA PROTECTION

Name of Faculty Member/University

Address

_____

_____

_____

Ljubljana, _____

No.: _____

I, the undersigned,_____, born on_____, residing at _____

_____, member of the commission (panel, etc.)_____,

aware of the nature of personal data that I will collect, edit, process, change, store, disclose or use in my work as a member of the University of Ljubljana (Member Faculty) commission (panel, etc.), hereby

D E C L A R E

to safeguard all personal data encountered during my work as professional and business secrecy.

I, the undersigned, have been instructed and am aware that the disclosure of the personal data encountered during my work to unauthorised persons or the abuse of such data is sanctioned as a criminal offence and is, at the same time, a reason for immediate dismissal of membership in a University of Ljubljana body.

Signature:

_____

Sample form 3

POWER OF ATTORNEY
SAMPLE FORM

Name of Faculty Member/University

Address

_____

_____

_____

_____(- responsible person)

Ljubljana, _____

No.: _____

Based on the provisions of the Rules on the protection of personal and confidential data at the University of Ljubljana, I, as at _____,

AUTHORISE

the employee_____, born on_____, residing at_____, employed at the post_____, to process the personal data of _____(students, employees, other, etc.) kept in the following personal data collections:

1. _____
2. _____
3. _____

This power of attorney shall apply until it is withdrawn.

(Stamp)

Signature of the responsible person:

_____

To be delivered to:

- the HR Management Office,
- the principal,
- the archives of powers of attorney for personal data management

Sample form 4

SAMPLES OF RECORDS OF PERSONAL DATA DISCLOSURES BY FACULTY MEMBERS OR THE UNIVERSITY OF LJUBLJANA

Name of Faculty Member/University

Address

_____

_____

_____

Ljubljana, _____No.:

_____

1. RECORD OF THE REMOVAL OF PERSONAL DATA MEDIA FROM BUSINESS PREMISES

Date of removal	Reason for removal	Purpose of removal	Approval	Date of return	NOTES

2. RECORD OF THE COPIES MADE OF THE CONTENTS OF PERSONAL DATA COLLECTIONS

Date of copy-making	Type of collection copied	The purpose for which copies are used	Place of storage for copies	Date of last update to a copy	Date of destruction of copy	NOTES

3. RECORD OF THE PERSONS INFORMED OF DATA DISCLOSURE

Date of request	Basis for the request	Institution	Name and surname of the	Employee who disclosed	Date of data disclosure	Date of informing the person	Person's signature	NOTES

			person subject to data disclosure	the data		of data disclosure	on learning about data disclosure	

4. A RECORD OF PERSONS AUTHORISED TO COLLECT, EDIT, USE, DISCLOSE AND STORE PERSONAL DATA AND WITH ACCESS TO PERSONAL DATA USING PASSWORDS

Name and Surname	Job post	Type of personal data processing	Type of personal data or collection	Date of power of attorney	Date of withdrawal of the power of attorney:	NOTES

5. A RECORD OF ALTERATIONS AND UPDATES TO THE SYSTEM AND APPLICATION SOFTWARE

Date of software modifications	Type of software modifications	Name and surname of the person carrying out modifications	Purpose of the modification	The person's signature	NOTES

6. A RECORD OF THE PERSONS INFORMED OF THE CONTENT OF THE RULES ON THE PROTECTION OF PERSONAL AND CONFIDENTIAL DATA

Name and surname	Job post	Date of informing	Person's signature	NOTES