Date: 6. 6. 2023

Guidelines
for Processing and Protection of Personal Data at the University of Ljubljana School of Economics and Business (SEB LU)

Legal Basis:

- Higher education act (ZviS),
- Personal Data Protection Act-2 (ZVOP-2),
- Regulation on the Protection of Personal and Confidential Data at the University of Ljubljana,
- official opinions and decisions of the Information officer,
- General Data Protection Regulation of the European Union (hereinafter referred to as GDPR).

1. **General Legal Basis for Processing Personal Data:**

The general legal basis for permissible processing of personal data (hereinafter referred to as PD) is determined in **Article 6 of the Personal Data Protection Act (ZVOP-2)**. PD can only be processed if the processing of data and the PD being processed are determined by law, or if the processing of specific PD is based on the individual's personal consent or any other legal basis which derives from ZVOP-2.

The relevant article of ZVOP-2 specifically regulates the legal basis for processing PD in the public sector, which includes public universities (public institutions). In the public sector when performing administrative or official duties, PD can only be processed if prescribed by law, which may also require that certain PD be processed only based on the individual's personal consent. In other cases, the applicable legal bases are defined by the provisions of ZVOP-2 or by the GDPR.

2. **Principle of Proportionality and Types of PD Records Processed at SEB LU:**

When processing PD, the principle of proportionality must be considered, which is one of the fundamental principles to be followed in processing PD. It stipulates that the PD being processed must be relevant and appropriate in scope for the purposes for which they are collected and further processed. The purpose of processing PD must be specified by law, and in the case of processing based on an individual's personal consent (or any other legal basis), the individual must be informed in writing or by other appropriate means about the purpose of processing personal data (article 12 of the GDPR). The Higher Education Act (ZViS), as a special law, specifies to whom and in what manner SEB LU can disclose students' personal data and for what purpose. ZViS in Article 81 determines the list of records containing students' personal data, and subsequent articles prescribe other records required by the law itself at UL EF.

3. **Purpose of Processing Students' PD**:

The purpose of processing students personal data is precisely defined, namely, to collect, process, store, and disclose students' PD from the records specified in Article 81 of ZViS for the needs of our educational, scientific research, artistic, professional, and library activities. All records established by lecturers for their subjects: partial grades, seminar papers, study practice, etc. are processed until the purpose of maintaining such records exists, which means when a student graduates or finishes an exam for a specific subject, there are no longer reasons or purposes to store such personal data.

All legal records of former students are maintained and stored by the Student Affairs Office and Archive of SEB LU for the needs of state authorities, local community authorities, holders of public authority, and student organizations related to the realization of students' rights under specific regulations. **Personal data may be used and published for statistical analysis only if the student's identity is not identifiable (i.e., if anyone needs personal records for later use, it is necessary to anonymize the personal data of former students).**

4. **Protection of PD:**

The areas where protected PD holders are located - every document containing personal data and every other computer or electronic data carrier - as well as the hardware and software (referred to as security areas in the text), must be protected by organizational, physical, and technical measures that prevent unauthorized access to data.

Currently, locking offices/cabinets when they are empty, accessing personal computers via usernames and passwords, sharing shared files in a password-protected manner, and implementing a clean desk policy (i.e., storing documents containing PD in locked cabinets and not on desks when not in use) are considered sufficient security measures.

Processing PD on official computers outside the premises of the SEB LU is permitted, but employees **must ensure that unauthorized individuals do not access this data** (particularly emphasizing the protection of official computers from theft and access to the computer should be password protected).

Personal data may only be transferred using information technology, telecommunications, and other means while implementing procedures and measures that prevent unauthorized persons from appropriating or destroying the data or gaining unauthorized access to its content.

5. **SPECIAL CATEGORIES OF PERSONAL DATA and the transmission of personal data:**

SPECIAL CATEGORIES OF PERSONAL DATA include data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, criminal records, or offenses, as well as biometric data. If any sensitive personal data are sent or forwarded by SEB LU (**assuming on a valid legal basis**), protective mechanisms should be employed (e.g., sealed envelopes requiring a signature upon receipt, password-protected USB drives, password-protected email with a password transmitted through another channel, etc.).

Personal data should be sent by registered mail. The envelope used for transmitting personal data should be designed in such a way that the content of the envelope is not visible under normal light or illumination. Additionally, the envelope should ensure that opening it and accessing its contents cannot be done without visible traces of tampering.

All personal data can be transmitted via official email, but for sensitive and protected personal data, encryption should be used. Even for data that does not contain sensitive personal information, it is recommended to send them in encrypted files separate from the passwords used to open them. Passwords should be communicated to recipients in person.

Personal data should only be disclosed to third parties who demonstrate the appropriate legal basis or provide a written request or consent from the individual to whom the data pertains (e.g., social services, government authorities, the individual to whom the data pertains).

6. **Purpose of processing personal data:**

Personal data can only be kept in a personal data collection for as long as necessary to achieve the purpose for which the personal data are collected and processed. After the need to keep the personal data ceases, the data should be deleted or destroyed. This applies to personal data records stored on computers that are not archived or designated as permanent archival material (e.g., records of partial grades, records of grades for seminar papers, records of participation in New Year's parties, etc.).

7. **Specific examples of frequently asked questions regarding the processing of personal data:**

- Obtaining records of students through course websites (student numbers, names, surnames, enrollment, etc.) or from the registrar's office is possible for the purposes of conducting courses and academic activities (attendance at lectures/labs, seminar papers, other study-related tasks). It is necessary to ensure that the acquired personal data are not lost or otherwise accessed by unauthorized third parties. The amount of personal data collected should be minimized to what is necessary for carrying out the academic activities. Personal data should not be collected unnecessarily.

- Keeping records of partial grades, attendance, etc.: Ideally, relevant records should be managed through the Study affairs office. If that is not possible or if there is insufficient IT support, the records can be kept in physical form by each instructor who needs them for conducting the course. Sharing records with colleagues involved in the course is permissible (authorized employees of SEB LU), but further reproduction (copying and multiplying) is not recommended or allowed. Such records should be kept until the purpose is fulfilled, i.e., the completion of the course (once a student passes the exam for the course, there is no need to keep such records, and they should be deleted at the latest when the student finishes their studies).

- Conducting tests, exams: In the exam papers, students typically write their registration number, first name, last name, and then the teacher writes their grade. The physical copies of exams are kept for one year, as well as all other forms of knowledge assessment (Examination Rules of the SEB LU). **The storage and handling of exams containing two key identifiable personal data (name, surname, and registration number) should be done with utmost care.** It is necessary to prevent students from becoming acquainted with the exams of their colleagues. Exams are stored in locked cabinets, and during their transportation, a method of transfer should be ensured that prevents the loss of any of the exams.

- Viewing of tests, exams: It is crucial to prevent students from familiarizing themselves with the exams of other students, as they could easily obtain the registration number and full name of their fellow students. During the viewing process, only the written work of the respective student should be handed to them, and then they can share it with their present colleagues.

- Seminar papers: The retention period is the same as for exam papers - one year (SEB LU Examination Rules).

- Are the grades I transmit to the administrative office personal data? YES, if the record of grades includes the student's name, surname, and registration number. If you are sending records with all the aforementioned personal data of the student, **it is recommended to send them in an encrypted file to the administrative office**. We suggest submitting lists of grades with only registration numbers of students. The registration number prevents unnecessary disclosure of personal data, and only the respective student to whom the grade pertains should be informed, and no one else.

- Is it permissible to publish a student's registration number alongside the grade? YES, but it is necessary to protect the personal data of students in such a way that unauthorized persons cannot link

the personal names and surnames to the registration number. **On the other hand, publishing both the registration number and the full name of the student undoubtedly violates the provisions of the Personal Data Protection Act (ZVOP-2),** for which fines are imposed according to the rules of misdemeanor and inspection procedure.

- Is the publication of individual student schedules of teaching obligations on the electronic notice board in compliance with the provisions of the Personal Data Protection Act (ZVOP-2) and GDPR regulations? The Higher Education Act stipulates that SEB LU can process personal data of students "for the purposes of higher education activities," which, according to the Commissioner's opinion, is a broad definition that should be interpreted restrictively, taking into account the principle of proportionality. The mere mention of a student's first name and last name may not necessarily be considered protected personal data since an individual is not necessarily identifiable based solely on that information. However, other data are also published along with the first name and last name. Publishing individual student schedules of teaching obligations on the electronic notice board is not in line with the principle of proportionality (unless the website is password-protected), but such publication is acceptable on the physical notice board of SEB LU, where only a limited number of people can access the personal data. The distribution of teaching obligations is an essential part of communication between the faculty and students, serving the "needs of higher education activities." Nevertheless, the Information Commissioner recommends that the publication of individual student schedules of teaching obligations on the (physical or electronic) notice board of SEB LU should be carried out in a way that minimizes the intrusion into the privacy of students, as the same goal can be achieved by milder methods (publishing schedules with registration numbers or, for example, by groups - all students with surnames starting from A to C...).

- Is it permissible to process personal data based on the individual's personal consent? SEB LU can process personal data based on the individual's personal consent only when it does not involve performing administrative or official duties prescribed by law. In all other cases, the legal basis is mandatory and restrictive. Therefore, **personal consent cannot exclude or exceed the scope or purpose of processing personal data as determined by the law when it involves the exercise of powers granted to the controller in the public sector**.

- Is it permissible to disclose individual students' grades to other students? To disclose the grade of an individual student to another student, the student must authorize their "colleague" to have the teacher share their grade for viewing (the same applies to disclosing grades via email, where particular caution is required—namely, the identities of the requesting student and the authorizer must be unquestionably verified. If you are unsure, it is better to avoid such disclosure and invite the students for in-person viewing).

- Is it permissible to publish lists of students on classroom doors, notice boards at SEB LU, or the SEB LU website? We suggest publishing lists only with registration numbers or by grouping surnames (from A to N and from N to Ž).

- Is communication with students via email allowed? Communication with students via email is permitted and appropriate, provided that SEB LU has obtained all necessary consents from the students. However, the communication should relate to matters connected to the activities of SEB LU (education, pedagogical activities, study proces), and it should take place either through the study informatics system or the students' digital identities. Communication to private email addresses of students is possible if the addresses have been provided by the students themselves (implicit consent to be informed about the needs and progress of the study process, such as by completing a form, entering it into a record, or sending an email by the student). **However, exporting private email**

addresses of students from the Student Affairs Office for the purpose of communication by individual teachers is not possible. Communication with students about matters not strictly related to the subject but of interest to them (e.g., events outside the curriculum, student job inquiries, events organized by students themselves, etc.) **should focus on notice boards or other mass communication methods that do not involve sending emails to individuals** (such as informing all students through the Student Affairs Office, notice boards, or study informatics).

If a student initiates contact via email (asking questions, inquiries, etc.), it is merely regular correspondence to which the student has consented (implicit action - they sent you an email). In such cases, caution should be exercised regarding the disclosure of personal data (if they request you to provide any personal data, their own or that of another authorized colleague), as the identity of the student based solely on email is not absolutely verifiable (someone could impersonate the student and use their private, non-UL email with the student's data). Therefore, in such cases, it is advised to invite the student, who is requesting personal data, to visit office hours, where you can verify their identity in person.

- Is it permissible to publish information about the defense of a final thesis on the internet? The provisions of the University of Ljubljana Statute regarding examinations are also applicable to other forms of knowledge assessment (where defense is one of them). Therefore, the provisions on the public nature of oral exams apply analogously to the defense. The Information Commissioner believes that the purpose of public defense of final theses is different, so internet publication of defenses is permissible. However, the Information Commissioner warns that SEB LU can ensure greater protection of students' personal data with less intrusive measures (such as preventing website indexing).

- Is it permissible to publish students' personal data in a student yearbook? The publication of personal data of individual students in a student yearbook requires their personal consent. If a student provides their personal data for publication in the yearbook, the disclosure of personal data by a student is considered their personal consent if the student has been informed in advance that their personal data will be shared for publication in the yearbook and is aware of other information related to such publication, as well as the voluntary nature of providing such data. **Even for the publication of only the student's name and surname in the yearbook, their personal consent is required.** The yearbook may include the personal data of teachers associated with their employment as public servants, specifically their name, surname, and academic title. However, their photographs, for which individual consent from the teacher must be obtained, should not be published.