



## **Guidelines for the Processing and Protection of Personal Data at the University of Ljubljana School of Economics and Business**

### **1. General Legal Basis for the Processing of Personal Data**

The general legal basis for the lawful processing of personal data (PD) at the University of Ljubljana School of Economics and Business (UL SEB) is defined in Article 6 of the Personal Data Protection Act (hereinafter: ZVOP-2). Accordingly, PD may only be processed if such processing is prescribed by law or if the individual has given explicit consent for the processing of specific PD. Further in the same article, ZVOP-2 precisely defines the legal basis for PD processing in the public sector, which includes public universities (public institutions). In the public sector, PD may only be processed if prescribed by law, which may also specify that certain PD may be processed solely based on the individual's consent.

### **2. The Principle of Proportionality and Types of PD Records Processed by the University of Ljubljana**

The processing of PD should take into consideration the principle of proportionality, which is one of the fundamental principles, stating that the PD being processed must be appropriate and limited in scope relative to the purposes for which they are collected and further processed. The purpose of PD processing must be defined by law, and in the cases where processing is based on an individual's consent, the individual must be informed in advance, in writing or through another appropriate means, about the purpose of processing their personal data.

The Higher Education Act (ZViS), as a specialised law, defines to whom and in what manner UL SEB may disclose students' personal data, as well as the purposes for which such data may be used.

Article 81 of the ZViS specifies the list of records containing students' personal data, while subsequent articles define additional records that the law mandates UL SEB to maintain.

### **3. Purpose of processing a student's personal data**

The purpose of processing students' personal data is clearly defined, namely that student PD, as specified in the records outlined in Article 81 of the Higher Education Act, is collected, processed, stored, and shared for the purposes of our pedagogical, scientific-research, artistic, and professional activities, as well as library services (this also includes records created by lecturers for the purposes of their courses, such as partial grades, seminar papers, and study placements. HOWEVER, this processing only continues as long as there is a legitimate reason for maintaining such records. This means that once a student graduates or, at the latest, once they have completed the exam for a specific course, there is no longer any reason or purpose for storing such personal data.)

All legal records concerning former students are maintained and stored by the Student Affairs and Archive Department of UL SEB, for the purposes of state authorities, local government bodies, public authorities, and student organisations, related to the exercise of student rights under specific regulations. In the creation of statistical analyses, personal data may be used and published in a manner that ensures the student's identity is not identifiable (i.e., if anyone requires their own records at a later date, the personal data of former students must be anonymised.)

### **4. Safeguarding PD**

Premises where PD information is located—every document containing personal data and any other computer or electronic data storage medium—as well as hardware and software (hereinafter referred to as security areas), must be protected with organisational, physical, and technical measures that prevent unauthorised persons from accessing the data.

Currently, the appropriate security measures include locking offices/cabins when they are empty, access to personal computers via usernames and passwords, sharing shared files in a way that they are password-protected, and the clean desk policy. This means that documents containing PD are stored in locked cabinets and not on desks (when not in use).

The processing of PD on work computers outside the UL SEB premises is permitted; however, employees must ensure all measures are taken to prevent unauthorised persons from accessing the data (particular attention must be given to protecting work computers

from theft).

PD may only be transferred using information, telecommunications, and other means when procedures and measures are in place to prevent unauthorised persons from acquiring, destroying, or improperly accessing the data and its content.

## **5. Special categories of PD and data transfer**

Special categories of PD include data on racial or ethnic origin, political, religious, or philosophical beliefs, trade union membership, health status, sexual life, registration or removal from criminal or misdemeanour records, and biometric characteristics. If any sensitive PD is sent or transferred by UL SEB (assuming a valid legal basis), it is transmitted using protective mechanisms (e.g., to recipients in sealed envelopes with a delivery receipt, password-protected on a USB stick, password-protected via email—with the password sent through a separate channel, etc.).

PD must be physically sent by registered mail. The envelope containing the PD must be designed in such a way that the contents of the envelope are not visible under normal light or when illuminated with a standard light source. Furthermore, the envelope must ensure that it cannot be opened, and its contents accessed without visible signs of tampering.

Through official email, all PD can be sent. However, when dealing with sensitive PD, such transmission must be carried out in a way that the PD is encrypted, or the records containing such data, even if they do not contain sensitive PD, must be sent in encrypted files, which should be separate from the passwords needed to open them. The passwords are communicated to recipients personally.

PD are only forwarded to third parties who provide appropriate legal grounds or written requests or consent from the individual to whom the data pertains (e.g., Social Work Centres, state authorities, or the individual concerned).

## **6. Purpose of processing PD**

PD can only be kept in a personal data collection for as long as necessary **to achieve the purpose** for which the data was collected and maintained. Once the need to keep the PD has ceased, the data must be deleted or the data carriers destroyed. This applies to PD records stored by employees on their computers that are not archived or designated as

permanent archival material (e.g., partial grade records, seminar paper grade records, attendance records for a New Year's party, etc.).

## **7. Individual examples of the most frequently asked questions related to the processing of PD**

**The collection of student records through course records (enrolment numbers, names, surnames, enrolment details, etc.) or from the departmental student office** is allowed for the purposes of course delivery and academic activities (attendance at lectures/exercises, seminar papers, other assignments related to studies). It is necessary to ensure that the personal data obtained is not lost or otherwise exposed to unauthorised third parties. The scope of collected data should be kept to a minimum, only as much as needed for the academic activities. Personal data is not collected in excess (only that which is absolutely necessary).

**Record-keeping—partial grades, attendance, etc.:** The relevant records are maintained by the Student Affairs Department. If, due to the method of course delivery, this is not possible, or if it is not feasible due to inadequate informational support, the records may also be kept in physical form by each teacher who requires them for course delivery. Sharing records with course collaborators is allowed, provided they are employees of UL SEB. However, further reproduction (copying and duplication) is not allowed. Such records are maintained for as long as necessary to fulfil their purpose, i.e., until the course is completed (when the student passes the exam for the course, there is no longer a need to maintain such records). The records are deleted at the latest when the student finishes their studies.

**Conducting Tests, Exams:** On exam papers, students typically write their enrolment number, name, surname, and grade. Exams are stored in physical form for one year, as are all other forms of knowledge assessments. The storage and handling of exams that contain two key personal data points (name and surname, and enrolment number) is done with care, with particular attention paid to preventing students from seeing the exams of their peers. Exams are stored in locked cabinets, and during transfer, appropriate measures are taken to ensure that no exam can be lost.

**Viewing of Tests, Exams:** It is crucial to prevent students from seeing the exams of other students, as they could otherwise easily obtain the enrolment number and name and surname of their peers. During the viewing, only the student's own written work is handed to them.

**Seminar Papers:** The retention period is exactly the same as for exam papers—one year.

**Are the grades I send to the student office personal data?** Yes, if the record of the communicated grades also includes the student's name, surname, and enrolment number. If a record containing all the previously mentioned PD of the student is sent, it should be transmitted to the Student Affairs Department in an encrypted file, and the department will send the grade lists

with students' enrolment numbers. The enrolment number ensures that personal data is not unnecessarily exposed, and the grade is only shared with the individual student to whom it pertains

**Is it allowed to publish the student's enrolment number along with the grade?**

Yes, provided that the PD of the students are protected in such a way that individuals who are not authorised to process such data cannot link the names and surnames to the enrolment numbers. Conversely, publishing both the enrolment number and the student's name and surname is undoubtedly a violation of the provisions of ZVOP-2, for which a fine is foreseen, to be enforced according to the rules of misdemeanour and inspection procedures.

**Is publishing student assignment schedules on an electronic bulletin board in compliance with the provisions of ZVOP-2 and GDPR?** The Higher Education Act (ZViS) stipulates that UL SEB can process students' personal data "for the purposes of higher education activities." According to the Information Commissioner of the Republic of Slovenia, this is such a broad definition that it must be interpreted restrictively, taking into account the principle of proportionality. The mere fact of a student's name and surname is not necessarily considered protected personal data, as an individual may not be identifiable simply from their name. However, other data is often published alongside the name and surname.

Publishing named schedules of students' teaching obligations on an electronic bulletin board is not in compliance with the principle of proportionality (unless the internet or intranet page is password-protected). However, publishing such schedules on a physical bulletin board at UL SEB, where only a small circle of people can view the PD, is allowed. The distribution of teaching obligations is considered a mandatory form of communication between UL SEB and students, which serves the "needs of higher education activities."

Nevertheless, the Information Commissioner of the Republic of Slovenia recommends that the publication of named student teaching schedules on (either physical or electronic) bulletin boards at UL SEB should be done in a manner that minimally infringes upon students' privacy. For instance, the School can achieve the same goal by publishing the schedule using enrolment numbers or grouping students (e.g., from surnames starting with A to C).

**Is it permissible to process personal data based on an individual's consent?** UL SEB can process PD based on an individual's consent only when it is not part of the execution of tasks carried out by the institution under legal authority. In all other cases, the legal basis must be defined by law. Therefore, individual consent cannot exclude or exceed the scope or purpose of PD processing as prescribed by law, especially when it pertains to the execution of powers granted to public sector entities.

**Is it permissible to share the grades of individual students with other students?** To share the grade of one student with another, the student must authorise their "peer" to allow the teacher

to disclose their grade for review. The same applies when sharing grades via email, where extra caution is needed. The identities of both the student requesting and the authorising student must be clearly verified. Otherwise, this type of sharing should be avoided, and the students should be personally invited to review the grade.

**Is it permissible to publish lists of students on, for example, classroom doors, bulletin boards at UL SEB, or the UL SEB website?** A list that only includes enrolment numbers or groups of surnames (e.g., from A to N and from N to Ž) is allowed.

**Is communication with students via email permitted?** Communication with students via email is allowed and appropriate, provided that UL SEB has obtained all necessary consents from the students. This applies as long as the students are informed about matters related to the activities of UL SEB (higher education activities), and such communication is carried out either through the student information system or through the students' digital identities. Communication to students' private email addresses is only possible if the relevant addresses have been provided by the students themselves, thereby giving explicit consent to be informed about the needs and progress of their studies. This can be done through completing a form, entering information into a record, or sending an email by the student, etc. The export of students' private email addresses from the Student Affairs Department for the purpose of communication by individual teachers is not allowed.

Communication with students about matters not strictly related to course delivery, but of interest to them: for example, regarding events outside the curriculum at UL SEB, inquiries about student work, or events organised by students themselves (e.g., a picnic...), communication should focus on the bulletin board/other mass communication methods that do not involve sending individual emails. Information for all students should be communicated through the Student Affairs Department, either via the bulletin board or student information system.

If a student contacts you via email (e.g., for questions, inquiries, etc.), this is considered ordinary correspondence, which the student has initiated with their explicit consent (by sending the email). In such cases, attention must be paid to the transmission of PD (if they want personal data to be shared, either their own or that of a colleague they wish to authorise). The identity of the student via email is not absolutely verifiable (someone could impersonate the student and use a private email rather than a UL SEB email). Therefore, in such cases, it is advised to invite the student to attend office hours in person, where you can verify their identity.

**Is it permissible to publish information about the defence of a thesis on the internet?** The provisions of the Statute of the University of Ljubljana concerning exams also apply to other forms

of knowledge assessment (with the thesis defence being one such form of assessment). Therefore, the provisions regarding the public nature of oral exams also apply to thesis defences. The Information Commissioner believes that the purpose of public access in the case of thesis defences is different, and thus, publishing information about the defence on the internet is permissible. Nonetheless, the Information Commissioner of the Republic of Slovenia warns that UL SEB can ensure greater protection of students' personal data with less intrusive measures (e.g., by disabling the indexing of web pages).

**Is it permissible to publish a student's personal data in a student yearbook?** To publish a student's PD in a student yearbook, their explicit consent is required. The transfer of PD by the student is considered their consent if the student has been informed in advance that their PD will be used for publication in the yearbook and is aware of the other relevant information regarding such a publication, as well as the fact that the submission of these data is voluntary. Even for the publication of just the student's name and surname in the yearbook, their explicit consent is required. The yearbook may include the PD of teachers related to the execution of their public service employment, i.e., their name, surname, and academic title, but not their photographs. For the publication of photographs, explicit consent from the individual teacher is required.

March 2025