

B3-02/2-SR



PALACKÝ UNIVERSITY IN OLOMOUC
RECTOR'S DIRECTIVE

B3-02/2-SR

Protection of Personal and Sensitive Data at Palacký University in Olomouc

Contents: Based on Act No. 101/2000 Sb., on the protection of personal data and on amendment to some other acts, as amended, the present Directive complements and specifies some of the provisions of the Act and defines organizational arrangements within UP.

Drafted by: Manager of the Legal Department of the Rector's Office

Date the Directive comes into force and effect: As of the date of publication

Date of publication: 31 January 2002

Distribution list: Rector, Vice-Rectors, Bursar, Rector's Office
Deans and Secretaries of Faculties
Manager of the Information Center of UP and Accommodation and Dining Facilities
Manager of the Economic, Technical-administrative and Operational and Management Departments of the Rector's Office
Legal Department and Inspection Department of the Rector's Office
Organization and Development Department of UP

Protection of Personal and Sensitive Data

at Palacký University in Olomouc

Article I Introductory Provisions

1. Based on Act No. 101/2000 Sb., on the protection of personal data and on amendment to some other acts, as amended, the present Directive complements and specifies some of the provisions of the Act and defines organizational arrangements within Palacký University in Olomouc (hereinafter "UP"). The Directive defines procedures for processing personal and sensitive data within UP and stipulates the rights and obligations of employees, students or, as the case may be, other individuals or legal entities taking part in activities related to the processing of such data.
 2. The Directive is issued in accordance with the provisions of Part VI, Articles 22 to 24 of the Internal Organization Code of UP.
 3. Personal data shall mean any data related to a specific or definable individual (hereinafter referred to as the "data subject"), i.e. the person whose identity may be directly or indirectly determined on the basis of one or more pieces of such data.
 4. The processing of personal data shall mean any systemic operations or series of operations with personal data regardless of whether they are automated or carried out by other means. Processing includes, but is not limited to, saving such data on information media, making them public or accessible, modifying or changing, searching for, using, keeping, exchanging, classifying or combining, blocking or destroying them as well as handing them over and spreading them.
 5. The present Directive protects all personal data processing carried out by UP employees and students within their work or study requirements or, as the case may be, by other individuals or legal entities that process personal data under a contract with UP (hereinafter referred to as "designated persons").
2. The following data shall constitute an exception to the prohibition under Paragraph 1 of this Article:
 - data on health entered in the records of employees and students if such data were provided for the record by the data subject voluntarily and are kept for his or her benefit (e.g. they may affect the admission to study, accommodation in university dormitories, or the assessment of taxes or other statutory payments),
 - data on membership in trade unions active at UP stated in the personal and pay records of employees if such data were provided by the data subject voluntarily for the purposes of the said records and are used for the payment of membership fees or other payments, including their entry in accounts,
 - data on the criminal records of UP employees and students if such data were provided by the investigating, prosecuting, and adjudicating bodies as part of the service of the sentence (e.g. prohibition to carry out an activity) or were referred for further proceedings (e.g. disciplinary penalties for UP students, penalties under the labour law for UP employees).
 3. Data under indents 1 and 2 of Paragraph 2 may only be processed subject to an express written consent by the data subject. It shall clearly follow from such a consent which data it applies to, for what purpose, in what extent, and for which period it was granted as well as who grants it to whom. By signing the consent the data subject also confirms that he or she has been advised of his or her rights, including, but not limited to, the option of revoking such a consent at any time.
 4. Designated persons who are responsible for entering and destroying such data in accordance with the nature of their processing under Article IV hereof shall retain such a consent for the whole period for which the data are processed.

Article II Sensitive Data

1. It is strictly prohibited to process sensitive data at UP; such data include data about the nationality, racial or ethnic origin, political opinions, membership in political parties or movements, trade union or employee organizations, religious or philosophical attitudes, criminal records, health, and sexual life of the data subject.

Article III Publication of Personal Data

1. Publication of personal data shall mean making the data accessible to undefined persons or groups of persons, in particular through the media or other public announcements, or by publishing them on a public list (e.g. on a public website).
2. Personal data protected under these provision may be made public only to the following extent:

- a) first name,
 - b) surname,
 - c) academic titles,
 - d) photograph,
 - e) post at UP,
 - f) position within the organizational structure of UP,
 - g) offices held at UP,
 - h) programs and fields of study followed at UP, including their type, form, and length of study,
 - i) contact details related to UP (workplace addresses, phone numbers, fax, e-mail addresses),
 - j) CV,
 - k) course of academic qualifications,
 - l) participation in individual forms of creative activities at UP (e.g. membership in specialized associations and their bodies, activities abroad, grants etc.),
 - m) publications,
 - n) courses taught at UP,
 - o) personal academic webpage.
3. Data subjects may determine the extent to which the data under d), j), m) and o) of Paragraph 2 of this Article are published, or may decide not to publish them at all.
 4. Data under Paragraph 2 may only be made public for data subjects who:
 - A. are employed by UP, or are working for UP under a similar contract,
 - B. are students at UP enrolled in study and their study has not been interrupted or terminated,
 - C. serve currently on any UP body,
 - D. are currently active at UP and may not be included under A) to C) (e.g. foreign persons within exchange stays).

**Article IV
Designated Persons**

1. Personal details exceeding the scope of Article III hereof may only be accessed by:
 - A. persons who are responsible for entering and destroying such data in accordance with the nature of their processing under Article I (4) hereof,
 - B. persons senior to persons under A) within the organizational or methodological hierarchy,
 - C. persons responsible for the organizational, functional, and technical administration of data processing (usually analysts, programmers, system and network administrators etc.),
 - D. other persons who are authorized to use such data to fulfill their work requirements in accordance with the nature of the data processing under Article III (usually heads of departments, sections, or divisions).
2. Designated tasks under Paragraph 1 may only be performed by persons who have been previously

acquainted with the Internal Organization Code of UP and other applicable legal regulations governing the field.

3. Persons may be designated to process data by a Vice-Rector determined by the Rector, the Bursar, Deans of individual faculties, the Manager of the Computer Center of UP, and the Manager of the Accommodation and Dining Facilities of UP, always within the scope of their powers. Should any dispute as to the powers arise, it shall be ultimately decided by the Rector of UP.
4. Persons defined in the previous paragraph shall determine in writing the specific persons authorized to process personal data, and update the list of designated persons in relation to all persons authorized to process the respective database.
5. Designated persons shall always process personal data only to the extent of the nature of the respective data processing under Article VI hereof.
6. Designated persons shall keep personal data and security measures, the disclosure of which may compromise the security of the personal data, confidential. The duty of confidentiality survives the termination of employment or study, or completion of contracted tasks.

**Article V
Personal Data Security**

1. Written documents and other information media of UP which contain personal data protected hereunder shall be kept in lockable cabinets at UP workplaces or, as the case may be, other secure places according to the nature of the respective data processing under Article VI, or shall be secured by encrypting.
2. Computers and other devices, on which documents containing personal data protected hereunder are saved, shall be secured against free access by unauthorized persons, usually by means of passwords, encrypting, or locking.
3. Copies of personal data protected hereunder shall be made on technical information media in accordance with the operation rules for individual data processing methods and shall be kept in lockable cabinets at UP workplaces or, as the case may be, other secure places according to the nature of the respective data processing under Article VI, or shall be secured by encrypting. As a matter of principle, the copies shall always be kept in rooms other than those where the original data are kept.

**Article VI
Personal Data Processing Entry and Records**

1. UP constituent parts (or, as the case may be, employees and students), that are going to process

personal data protected under this provision, or want to change the existing way of personal data processing, shall inform the Rector's Office thereof.

2. Notification under Paragraph 1 of this Article shall include a complete description of the respective data processing with the following details:
 - a) the purpose of processing,
 - b) the extent of the processed data,
 - c) the class of the data subject and personal details related to the subject,
 - d) the sources of the personal data,
 - e) a description of how the personal data are to be processed, including the determination of liability of the individual designated persons, jobs, or workplaces in charge of individual phases of the processing,
 - f) the recipients or classes of recipients that might have access to such data or that will receive them,
 - g) the method for obtaining the consent of the data subjects to have their personal data processed,
 - h) the method for informing data subjects that certain data have been collected about them,
 - i) the method for verifying that the personal data are true and accurate,
 - j) the method of informing data subjects that their personal data that are processed,
 - k) the expected transfers to other countries,
 - l) a description of measures to secure personal data,
 - m) the guarantor in charge of the respective workplace,
 - n) the connection to other administrators or, as the case may be, data processors.
3. The Rector's Department (a designated employee of the department) shall compile the submitted documents and draw up a respective notification on their basis, which shall be sent to the Office for Personal Data Protection (hereinafter the "Office") in accordance with the provisions of Section 16 et seq. of Act No. 101/2000 Sb., on the protection of personal data and on amendment to some other acts, as amended.
4. Applicants may start processing personal data, or change the method of their processing, only after they have received a consenting opinion from the

Rector's Department. A consenting opinion under Sentence 1 of this Paragraph is issued upon the registration of the notification under Paragraph 3 of this Article.

5. The Rector's Department shall keep records of any personal data processing at UP to the minimum extent defined in Paragraph 3 of this Article.

Article VII

Information about Personal Data

1. Information on UP is classified in accordance with the Internal Organization Code of UP according to the recipients of the data:
 - a) information intended for the public,
 - b) information intended for UP employees and students,
 - c) information intended only for selected UP employees.
2. Personal and sensitive data are included under Paragraph 1 (c) of this Article. Such information includes, but is not limited to, information of a professional nature, information on the personal and pay conditions of UP employees, information about UP students and any other information defined by generally applicable legal regulations.
3. Information on personal and sensitive data is provided in oral, written, or electronic form or, as the case may be on the official notice boards of UP constituent parts, but only to the extent defined by Act No. 101/2000 Sb., the Internal Organization Code and this Directive.

Article VIII

Final Provisions

1. All UP employees who process personal and sensitive data or get into touch with such data are responsible for the compliance. Managers carry out regular inspections of the compliance with the protection of personal and sensitive data regulations in accordance with the internal inspection system implemented at UP as defined by the Internal Organization Code of UP.
2. The present Directive comes into force and effect on the date it is published.

In Olomouc on 31 January 2002

Prof. MUDr. PhDr. Jana Mačáková, CSc., in her own hand,
Rector of UP