University of Chemistry and Technology, Prague

Title	INTERNAL REGULATION No. A/N/961/3/2018
Subject	**Protection and Processing of Personal Data at the University of Chemistry and Technology, Prague**
Applicability	All university
Effective from	21 May 2018
Effective to	Unlimited
Revision	-
Cancelled	Decree No. 30.18/03 on Protection of Personal Data at UCT Prague
Prepared by	Bursar's secretariat – 962
Issued by	Prof. Ing. Karel Melzoch, CSc., Rector

This translation is provided for convenience only. The Czech version is the legally binding version. In case of any inconsistency or ambiguity, the Czech version shall prevail.

PART ONE
Introductory provisions

Article 1
Basic provisions

(1) This internal regulation further specifies and regulates the principles and rules of personal data processing at the University of Chemistry and Technology, Prague (hereinafter referred to as 'UCT Prague'), regulates the basic processes and processing of personal data as well as rules for the acquisition, collection, storage, use, dissemination and retention of personal data. This internal regulation establishes the responsibilities of individuals tasked with ensuring the protection of personal data and defines the rights and obligations of employees, students and other affected natural and legal persons.

(2) This internal regulation is binding also for natural and legal persons who have another legal relationship to UCT Prague.

(3) This internal regulation is based on Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as the 'GDPR') and related legal regulations.

Article 2
Definitions of basic terms

(1) This internal regulation has adopted terms used in the GDPR. This Article includes a list of basic terms; the definitions of other terms used in connection with personal data protection are provided in Article 4 of the GDPR.

(2) The term ‘personal data’ refers to any information about an identified or identifiable natural person (hereinafter referred to as the ‘Data Subject’). A Data Subject is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Data Subject.

(3) The term ‘personal data processing’ refers to any operation or set of operations with personal data or sets of personal data that are carried out with or without the help of automated processes such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(4) The term ‘controller’ refers to a natural or legal person, a public authority, an agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union or Member State law, such law may specify the controller in question or set out the criteria for its designation.

(5) The term ‘processor’ refers to a natural or legal person, a public authority, an agency or another body which processes personal data for the controller. In certain cases, UCT Prague may take on the role of processor.

(6) The term ‘recipient’ refers to a natural or legal person, a public authority, an agency or another body to whom the personal data are disclosed, whether it is a third party or not. However, public authorities which may obtain personal data in the framework of a particular inquiry in accordance with the law of a Member State shall not be regarded as recipients; the processing of such personal data by those public authorities must be in compliance with the applicable data protection rules for the given purposes of the processing.

(7) The term ‘third party’ refers to a natural or legal person, a public authority, an agency or another body which is not a data subject, a controller, a processor nor a person under the direct authority of the controller or processor who is authorised to process personal data.

(8) The term ‘consent of the data subject’ refers to any free, specific, informed and unambiguous expression of the data subject’s will by which they, by a statement or by a clear affirmative action, gives consent to the processing of their personal data.

(9) The term ‘personal data breach’ refers to a breach of security leading to an accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to transmitted, saved or otherwise processed data.

(10) The term ‘filing system’ refers to any structured set of personal data accessible according to specific criteria, whether centralised, decentralised or divided based on functional or geographical basis.

(11) The term ‘health status’ refers to personal data relating to the physical or mental health of a natural person, including data on the provision of health services, which reveal information about that person’s health status.

PART TWO
Responsibility of UCT Prague

Article 3
Division of responsibility

(1) The Rector of UCT Prague (hereinafter referred to as the 'Rector') is responsible for compliance with principes, rules and procedures relating to the processing of personal data outside and inside of UCT Prague in cases carried out at the central level of UCT Prague and in areas in which responsibility has not been transferred to another person in accordance with this Article.

(2) The Bursar is accountable to the Rector for compliance with principes, rules and procedures relating to the processing of personal data carried out within the areas of their authority as defined in Article 13 of the internal regulation 'Statute of UCT Prague' (hereinafter referred to as the 'Statute'), Article 19 of the internal regulation 'Organisational Rules of UCT Prague' (hereinafter referred to as 'OR') and other internal regulations of UCT Prague.

(3) Vice-rectors are accountable to the Rector for compliance with principes, rules and procedures relating to the processing of personal data carried out within the areas of their authority determined by the Rector and as defined in Article 8 of the Statute, Article 18 of OR and other internal regulations of UCT Prague.

(4) The director of the Administration of University Facilities of UCT Prague (hereinafter referred to as 'AUF') is accountable to the Rector for compliance with principes, rules and procedures relating to the processing of personal data carried out within the areas of their authority as defined in Article 18 of the Statute, Article 20 of OR and other internal regulations of UCT Prague. The director of AUF is also responsible for compliance with principes, rules and procedures relating to the processing of personal data carried out by employees of AUF, or other natural or legal persons that process personal data based on an agreement with AUF.

(5) The director of Technopark Kralupy of UCT Prague (hereinafter referred to as 'Technopark') is accountable to the Rector for compliance with principes, rules and procedures relating to the processing of personal data carried out within the areas of their authority as defined in Article 16 of the Statute, Article 20A of OR, the internal regulation 'Statute of Technopark Kralupy of UCT Prague' and other internal regulations of UCT Prague. The director of Technopark is also responsible for compliance with principes, rules and procedures relating to the processing of personal data carried out by employees of Technopark, or other natural or legal persons that process personal data based on an agreement with Technopark.

(6) The deans of individual faculties of UCT Prague are accountable to the Rector for compliance with principes, rules and procedures relating to the processing of personal data carried out by employees and students of faculties of UCT Prague, or other natural or legal persons that process personal data based on an agreement with faculties of UCT Prague in matters entrusted to them under the provision of Section 24 of Act 111/1998 Coll., on Higher Education Institutions and Amendments and Supplements to Some Other

Acts (Higher Education Act), as amended (hereinafter referred to as the 'Higher Education Act'), Article 15 of the Statute, Article 21 of OR and other internal regulations of UCT Prague.

Article 4
Personal data processing Coordinator

(1) Persons specified in Article 3, Paras 1 through to 6 must appoint a personal data processing Coordinator (hereinafter referred to as the 'Coordinator'), consisting of at least one person, in accordance with the structure given in OR in the following manner:
   a. The Rector in cases of personal data processing affecting the entire UCT Prague and the central university departments and Rector's Office departments that are directly subordinate to the Rector in accordance with Annex No. 3 to OR;
   b. The Bursar in cases of personal data processing affecting the central university departments and Rector's Office departments that are directly subordinate to the Bursar in accordance with Annex No. 3 to OR;
   c. The vice-rectors in cases of personal data processing affecting the central university departments and Rector's Office departments that are directly subordinate to the vice-rectors in accordance with Annexes No. 2 and 3 to OR;
   d. The director of AUF in cases of personal data processing affecting the central university departments and AUF departments that are directly subordinate to them in accordance with Annex No. 3 to OR
   e. The director of Technopark in cases of personal data processing at Technopark;
   f. The deans of individual faculties in cases of personal data processing at faculty departments that tare directly subordinate to them in accordance with Annex No. 1 to OR.
(2) The Coordinator is accountable to the persons referred to in Para 1 for compliance with the principles, rules and procedures relating to the processing of personal data carried out within the areas of their authority, and they work in close cooperation with the Data Protection Officer.
(3) The Coordinator is responsible for the activities referred to in Para 2 from the date of their appointment until the conclusion of such activities, including ensuring the archiving of data.
(4) Within the area of their authority, the Coordinator shall conduct an assessment of the impact of intended processing operations on the protection of personal data; for this purpose, they may request a written opinion from the Data Protection Officer.
(5) The persons referred to in Para 1 shall inform the Data Protection Officer of the appointment of a Coordinator without undue delay.
(6) In the case of personal data processing systems that already exist, a Coordinator shall be appointed by the persons referred to in Para 1 within 2 months from the effective date of this internal regulation. For new personal data processing systems, a Coordinator shall be appointed prior to the commencement of personal data processing.

Article 5

Persons involved in personal data processing

(1) Other authorised persons that may be involved in specific operations related to personal data processing include in particular:
   a. Employees of UCT Prague when completing work tasks ensuing from their job description;
   b. Persons responsible for organisational, functional and technical administration of the given personal data processing (system administrators etc).
(2) The controller may appoint other persons that will participate in personal data processing.
(3) Persons involved in personal data processing must carry out the personal data processing only to the extent strictly necessary and within the scope of their assigned work task.
(4) Persons involved in personal data processing must maintain confidentiality regarding personal data and security measures, the publication of which could compromise the security of personal data.
(5) Persons involved in personal data processing must monitor the updates of internal regulations of UCT Prague concerning the processing and protection of personal data.

Article 6
Personal data processing in final theses and other theses

(1) In cases where personal data are processed in final theses or other academic works (Bachelor's, Master's, doctoral theses etc), the supervisor or the relevant employee of UCT Prague must inform the author of the thesis about their obligations under this internal regulation and to ensure that any necessary steps are taken in accordance with this internal regulation. The supervisor or the relevant employee of UCT Prague is entitled to request an opinion from the Data Protection Officer.

Article 7
Personal data processing within scientific, research, development, innovation, artistic and other creative activity at UCT Prague and supplementary activity at UCT Prague

(1) In cases where personal data of students and employees of UCT Prague are processed within their involvement in a project etc it is necessary to obtain the consent of these data subjects, unless another legal basis for the processing of such personal data exists.
(2) If personal data of third parties, or of employees or students of UCT Prague, are processed within UCT Prague's supplementary activity and there is no legal basis for such processing, it is necessary to obtain the consent of these data subjects.

PART THREE

Data Protection Officer

Article 8
Status of the Data Protection Officer

(1) The Data Protection Officer (hereinafter referred to as the 'DPO') reports to the Rector in accordance with OR.
(2) The DPO is appointed and dismissed by the Rector.
(3) The DPO is bound by confidentiality in connection with the performance of their duties.
(4) In accordance with the GDPR, UCT Prague is required to publish information about the DPO on the public section of its website.
(5) The persons referred to in Articles 3 through to 5 are required to provide the DPO with the cooperation necessary for the performance of their duties.
(6) UCT Prague shall appoint the DPO and ensure their status in accordance with Articles 37 and 38 of the GDPR.

Article 9
DPO's duties

(1) The DPO shall perform the following duties in particular:
   a. they provide information and advice to students and employees of UCT Prague who process personal data regarding their obligations under the GDPR, this internal regulation, and other generally binding legal regulations related to the protection of personal data;
   b. they monitor compliance with the GDPR, this internal regulation and other generally binding legal regulations related to the protection of personal data, including the allocation of responsibilities;
   c. they oversee the implementation of personal data protection and processing;
   d. they provide advice upon request regarding data protection impact assessments and monitor their implementation in accordance with Article 35 of the GDPR;
   e. they cooperate with the supervisory authority;
   f. they act as a contact point for the supervisory authority on matters relating to processing, including prior consultation under Article 36 of the GDPR, and engage in consultations on any other matters as necessary;
   g. they organise training for UCT Prague employees and responsible persons involved in the processing of personal data, and continuously strive to raise awareness regarding the principles of personal data protection and processing, as well as related audits;
   h. they handle objections raised by data subjects in accordance with Article 13 of this internal regulation;
   i. they work closely with Coordinators, receiving their inputs and proposals;
   j. following prior consultation with the persons specified in Article 3, they notify the supervisory authority of personal data breaches (Article 33 of the GDPR) and communicate personal data breaches to the data subject (Article 34 of the GDPR).

(2) The Rector may assign other tasks and duties to the DPO. None of these tasks or duties shall lead to a conflict of interests with the performance of the performance of their role as the DPO.

Article 10
Scope of work of the DPO at UCT Prague

(1) If the DPO identifies a risk of a breach of personal data protection rules, whether arising from the GDPR, the Act or an internal regulation, or if an actual breach is discovered, the DPO must, without undue delay, notify the Coordinator and the person responsible (as defined in Article 3 of this internal regulation) and provide a written recommendation to rectify the problematic or risky situation. The Coordinator is required to discuss the identified situation with the DPO within a reasonable timeframe; if they concur with the DPO's findings, they shall implement the recommended measures. If the Coordinator disagrees with the DPO's recommendation, they must provide the DPO with a written explanation detailing why they believe no breach has occurred or is at risk of occurring. This written justification shall be sent to the DPO and the person responsible in accordance with Article 3 of this internal regulation.

(2) In case there is a risk of breach of personal data protection rules arising from the GDPR or this internal regulation, or if a breach is identified and no controller has been appointed for the given area, the DPO will notify the responsible persons in writing in accordance with Article 3 of this internal regulation.

(3) The DPO must propose an adoption of general or individual measures in the area of personal data protection to persons specified in Article 3 of this internal regulation if:
   a. based on their findings in accordance with Para 1, they identify a risk of breach or breach of rules;
   b. it shall be appropriate in connection with the generalisation of practices in the area of personal data protection.

(4) Paras 1 through to 3 are without prejudice to the duties of the DPO in accordance with Article 9, Para 1, letter m) of this internal regulation.

PART FOUR
Data subject

Article 11
Rights of data subjects

(1) UCT Prague shall preserve the right of data subjects in particular to:
   a. information in accordance with Articles 12 through to 14 of the GDPR
   b. access to personal data in accordance with Article 15 of the GDPR
   c. rectification in accordance with Articles 16 and 19 of the GDPR
   d. erasure in accordance with Articles 17 and 19 of the GDPR
   e. restriction of processing in accordance with Articles 18 and 19 of the GDPR
   f. data portability in accordance with Article 20 of the GDPR
   g. objection in accordance with Article 22 of the GDPR

Article 12
Information provided to data subjects

(1) In accordance with Article 12 of the GDPR, UCT Prague in its capacity as the controller shall provide the data subject in a concise, transparent, intelligible, and easily accessible

form and using clear and plain language with all information specified in Articles 13 and 14 of the GDPR. Any communications regarding the processing of personal data, as required under Articles 15 through to 22 and Article 34 of the GDPR, shall be provided in the same manner.

(2) UCT Prague shall provide this information in electronic form in the public section of its website.

(3) Data subjects may contact the DPO regarding matters related to the processing of their personal data and the exercise of their rights under the GDPR and this internal regulation.

Article 13
Handling requests of data subjects

(1) The procedure and details for handling requests from data subjects exercising their rights are governed by the internal document 'Procedure for Handling Data Subject Application Settlement' (hereinafter referred to as the 'Procedure'), which is also published in the public section of the UCT Prague website.

(2) A data subject may lodge objections with the DPO regarding the procedure for handling a request or the manner in which it was handled.

PART FIVE
Principles relating to processing of personal data

Article 14
Principles relating to processing of personal data

(1) Principles relating to the processing of personal data are governed by Articles 5 through to 11 of the GDPR. When processing personal data, the following principles must be observed, according to which personal data must be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

(2) The persons specified in Articles 3 through to 5 of this internal regulation shall be responsible for, and be able to demonstrate compliance with, Para 1.

Article 15

Lawfulness of processing

(1) Processing of personal data at UCT Prague shall be lawful only if, in compliance with Article 6 of the GDPR, at least one of the following conditions is met and the processing is carried out only to the appropriate extent:
    a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
    b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    c. processing is necessary for compliance with a legal obligation to which the controller is subject;
    d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
    e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(2) Para 1, letter f) does not apply to the processing of personal data carried out by UCT Prague in cases where UCT Prague acts as a public authority in matters entrusted to it by law.

Article 16

Processing of personal data based on data subject's consent

(1) If there is no other legal basis for the processing of personal data, personal data may be processed only on the basis of the data subject's written consent to the processing.

(2) The data subject's consent must comply with the conditions set out in Article 7 of the GDPR, ie the consent must be given by the data subject in writing, it must be signed by the data subject, or it must otherwise be demonstrated that is has been given by the data subject, and the following must clear from the consent:
    a. Identity and contact details of the controller;
    b. Who is providing them;
    c. Which personal data the consent concerns;
    d. The period for which the consent is granted;
    e. Whether the personal data will be further transferred, and to whom;
    f. Advice on the rights of the data subject.

(3) The DPO shall keep a register of the used versions of consents to the processing of personal data.

Article 17

Processing of personal data for a purpose other than that for which data was collected

(1) In the event that UCT Prague intends to process personal data for a purpose other than that for which the data were collected and where the consent of the data subjects is lacking or the processing is not based on valid, generally binding legal regulations, the persons specified in Articles 3 through to 5 of this internal regulation are required to consult with the DPO regarding whether such processing is permissible under Article 6, Para 4 of the GDPR. Furthermore, the persons specified in Articles 3 through 5 of this internal regulation are required to provide the DPO with a written justification for this type of processing.

(2) The DPO will subsequently assess whether the processing of personal data for another purpose is in accordance with Article 6, Para 4 of the GDPR, taking into account, inter alia:

a. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and UCT Prague;
c. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 of the GDPR, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10 of the GDPR;
d. the possible consequences of the intended further processing for data subjects;
e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

(3) If the DPO concludes that the processing of personal data for another purpose in in accordance with the GDPR, they will make sure that the data subject is informed before the processing for another purpose commences.

Article 18
Processing of special categories of personal data

(1) Processing of special categories of personal data, which includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, shall be prohibited.

(2) Exceptions to the prohibition on processing of special categories of personal data are set out in Article 9 of the GDPR. Any processing of special categories of personal data by UCT Prague may take place only on the basis of one of the legal grounds listed in Article 9, Para 2) of the GDPR.

(3) Exceptions to the prohibition on processing of special categories of personal data at UCT Prague include in particular:

a. data concerning health status contained in employees' personnel files, for the purpose of fulfilling the controller's obligations arising from employment regulations;
b. data concerning students' health status, provided that such data were voluntarily submitted by the data subject within the scope of proceedings conducted by UCT

Prague pursuant to Section 68 of the Higher Education Act, and where such processing is necessary for the establishment, exercise or defence of legal claims within the meaning of Article 9, Para 2, letter f) of the GDPR;

c. data concerning students' health status, provided that such data were voluntarily submitted by the data subject, are processed on the basis of their explicit consent, and are maintained for the data subject's benefit (eg data affecting the course of the admissions procedure, data processed in the provision of services to persons with specific needs);
d. data regarding membership in trade union organisations active at UCT Prague, contained in employees' personnel files, provided that such data were voluntarily submitted by the data subject, are processed on the basis of their explicit consent and are used for the payment of membership dues or other contributions, including the accounting for such payments;
e. biometric data that allow for the direct identification of the data subject, based on the data subject's explicit consent;
f. data processed for the purposes of projects/research, based on the data subject's explicit consent.

(4) The processing of personal data as defined in Para 1, Para 3, letters c) through to f) may take place only based on an explicit consent of the data subject. This consent must be given in writing, signed by the data subject and it must clearly indicate what data it concerns, for what purpose, for what period and by whom it has been granted. By signing, the data subject also confirms that they have been informed of their rights in advance. The Coordinator is required to be able to demonstrate the existence of this consent throughout the entire period of data processing.
(5) Processing of personal data that does not require identification of the data subject is regulated by Article 11 of the GDPR.

Article 19
Termination of processing of personal data

(1) UCT Prague retains personal data only for the period necessary to achieve the purpose for which they are processed, including for archiving purposes.
(2) Once the purpose for processing personal data has ceased, or following the erasure of personal data upon the request of the data subject, the personal data shall be destroyed.
(3) The destruction of storage media containing personal data shall be carried out in a manner that prevents unauthorised persons from gaining accidental access to the personal data.

PART SIX
Register of processing of personal data at UCT Prague

Article 20
Registration and records of processing of personal data

(1) A register of the processing of personal data at UCT Prague (hereinafter referred to as the 'processing register') is established at UCT Prague to provide an overview of the

processing of personal data.

(2) The notification under Para 2 must contain a full characterisation of the given processing of personal data. The extent shall be set out in an internal regulation of UCT Prague.

(3) The proposer has the right to commence or change the existing processing of personal data only after they have received an official opinion from the DPO based on the outcome of the notification. If the opinion is negative, the matter will be consulted with the persons specified in Articles 3 through to 5 of this internal regulation.

PART SEVEN
Publication and protection of personal data at UCT Prague

Article 21
Publication of personal data

(1) Publication of personal data refers to making such data accessible to unspecified persons or groups of persons, mainly through mass media, other forms of public communication or as part of a public register (eg in the public section of the UCT Prague website). Making personal data accessible within UCT Prague's information systems is not publication.

(2) UCT Prague, unless the publication is prescribed by legal regulations in force, may publish personal data protected under this internal regulation only in the following extent:

a. First name, surname, academic titles
b. Job position at UCT Prague, placement within the organisational structure, roles held
c. Contact details in relation to UCT Prague
d. Process of academic qualification
e. Contribution to the different forms of creative activity
f. Publication activity
g. Teaching activities at UCT Prague

(3) The data subject has the right to choose the concrete scope of publication of personal data, such as a CV or photograph, or to choose that the data will not be published at all.

(4) The data specified in Para 2 may be published only for data subjects that are employed at UCT Prague, or for people who do not have an employment relationship with UCT Prague, but are currently active in the academic bodies of UCT Prague.

(5) In the case of the leadership of UCT Prague and its constituent parts, other individuals holding academic roles, or employees of UCT Prague for whom the publication of certain personal data follows from the nature of their job position, the publication of personal data shall be handled on an individual basis.

Article 22

Disclosure of personal data to third parties and processing of personal data by external processors

(1) In case UCT Prague as the Controller authorises an external processor to process personal data, a written agreement on processing of personal data must be concluded between UCT Prague and the processor, which must include the requirements pursuant to Article 28, Para 3 of the GDPR.

(2) The persons specified in Articles 3 through to 5 of this internal regulation are responsible for ensuring compliance with the correct procedure for disclosure of personal data to third parties outside UCT Prague in accordance with this internal regulation, the GDPR and generally binding legal regulations in force.

Article 23
Security of personal data

(1) UCT Prague must adopt and implement appropriate technical and organisational security measures, taking into account the nature, scope and purposes of the processing, to ensure the security of the personal data being processed and the compliance of such processing with the GDPR.

(2) Personal data must be kept in premises, locations, environments or systems accessible only to a pre-determined group of individuals, as designated by the persons specified in Articles 3 through to 5 of this internal regulation.

(3) Documents and mobile/external/portable technical data storage media UCT has at its disposal and that contain personal data protected under this internal regulation must be secured against unauthorised access, for example by being locked in cabinets or offices, or stored in other locations where their protection can be ensured in accordance with Paragraph 1. These same rules apply to copies of documents and other data storage media containing personal data.

(4) If personal data directly related to activities performed at UCT Prague (attendance sheets, notebooks etc) are processes, their security must be ensured by standard processes to prevent the risk of misuse of this personal data. Other obligations set out in this Article shall apply to the processing of such personal data only to the extent that complies with their nature and the circumstances under which they are typically processed.

(5) Computers and other technical equipment on which data containing personal data are stored must be secured against unrestricted access of unauthorised persons, in particular by passwords, encryption or locking.

(6) The rules and principles for the protection and processing of personal data in using the data network and computer systems at UCT Prague are set out in the internal regulations of the Computer Centre of UCT Prague.

PART EIGHT
Procedure in the event of a personal data breach

Article 24
Personal data breach

(1) A personal data breach is a state where a random or unlawful destruction, loss, alteration or unauthorised disclosure or publication of transferred, stored or otherwise processed personal data occur.
(2) In the event that persons specified in Articles 3 through to 5 of this internal regulation, or an employee of UCT Prague, become aware that a personal data breach might occur, they must notify the DPO immediately.
(3) Upon verifying the information, the DPO will assess whether the security breach constitutes, or is likely to constitute, a risk. In assessing the risks, the DPO will take into account, in particular, the category of personal data affected by the breach, the nature of the breach and the number of data subjects affected.
(4) In the event that the breach does not constitute such a risk, the DPO will only make a record of in the records of security breach incidents. If the DPO concludes that the security breach constitutes or may constitute a risk, they will immediately inform the persons specified in Articles 3 through to 5 of this internal regulation and will ensure this security incident is reported to the supervisory authority and possibly also the date subject.
(5) The DPO maintains records of all personal data breaches, which includes a description of the facts relating to each individual breach, the effects of the breach and the remedial measures taken.

Article 25
Reporting of a security breach

(1) The DPO will ensure that a security incident is reported to the supervisory authority without undue delay, but no later than 72 hours from the moment the security incident was notified to them. The report will include the information specified in Article 33 of the GDPR.
(2) If an obligation arises to notify a security breach incident to the data subject, ie if the security incident constitutes a high risk to the rights and freedoms of the data subject, and at the same time none of the conditions under which notification to the data subject is not required pursuant to Article 34, Para 3 of the GDPR are met, the DPO will notify the data subject of the personal data breach without undue delay, in the manner and to the extent prescribed by Article 34 of the GDPR.

Article 26
Remedial measures

(1) Following each personal data breach incident, the person designated in Articles 3 through to 5 of this internal regulation will adopt measures the purpose of which is to resolve the given breach and prevent its recurrence in the future. If the security breach constitutes a risk to the rights of the data subject, that person shall also take the necessary measures to mitigate any potential adverse impacts.

Prof. Ing. Karel Melzoch, CSc., m. p.
Rector