Rector's Directive No. 16/2018

To implement: Regulation (EU) No. 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)
Date of effect: 25 May 2018

Principles and Rules of Personal Data Protection

Part One – Fundamental Provisions

Article 1 – Subject-matter

1. This Rector's Directive ("the Directive") provides the principles and rules for processing of personal data at Charles University ("the University") and the responsibilities of persons ensuring personal data protection at the University, and defines the rights and duties of employees, students, and potentially also other natural or juridical persons involved in activities related to personal data protection.
2. This Directive is based on Regulation (EU) No. 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) ("the Regulation") and on Act No. 101/2000 Sb., on the protection of personal data and to change other laws, as amended ("the Act") where the Directive supplements and elaborates on some of the provisions of the Regulation and the Act governing the relations within the University and provides organisational procedures for their implementation.

Article 2 - Definitions

1. For the purposes of this Directive:
   a. "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one 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 natural person;
   b. "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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;
   c. "restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;
   d. "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
   e. "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational directive to ensure that the personal data are not attributed to an identified or identifiable natural person;
   f. "filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
   g. "controller" means the natural or legal person, public authority, agency or other 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
   h. "processor" means a natural or juridical person, public authority, agency or other body which processes personal data on behalf of the controller;
   i. "processors acting in a chain" means a situation when another person in the role of (partial) processor is involved in personal data processing based on a written consent of the University;
   j. "recipient" means a natural or juridical person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in

the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

k. “third party” means a natural or juridical person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
l. “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
m. “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
n. “genetic data” means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
o. “biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
p. “data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

2. Additional definitions are stated in Article 4 of the Regulation.

Article 3 – Principles Relating to Processing of Personal Data

1. Personal data must be:
   a. processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
   b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“purpose limitation”); further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
   c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
   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 (“accuracy”);
   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 (“storage limitation”); personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational directives required by the Regulation in order to safeguard the rights and freedoms of the data subject;
   f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational directives (“integrity and confidentiality”).
2. Persons stated in part two of this Directive are responsible for compliance with the principles under paragraph 1 and must be able to demonstrate, pursuant to Article 5 (2) of the Regulation, compliance with these principles (“accountability”).

Article 4 – Lawfulness of Processing

1. In accordance with Article 6 of the Regulation the processing is lawful only if and to the extent that at least one of the following applies:
   a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes (the conditions for consent are detailed in Articles 7 and 8 of the Regulation);
   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 in accordance with generally binding legal regulations in force and is necessary for compliance with a legal duty 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 in accordance with generally binding legal regulations in force and is necessary for the performance of a task carried out in the public interest or in 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. The provision of paragraph 1 (f) does not apply to processing of personal data carried out by the University when the University acts as a public authority in matters vested in the University by Act No. 111/1998 Sb., to regulate

higher education institutions, as amended (the Higher Education Act), or by another legal regulation. In such cases paragraph 1 (c) applies.

Article 5 - Processing of Special Categories of Personal Data

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited in cases to which paragraphs 2 and 3 do not apply.
2. Exceptions to the prohibition of processing of personal data under paragraph 1 are stated in Article 9 of the Regulation, in particular the personal data specified in paragraph 1 may be processed providing that the data subject has given explicit consent to the processing of such personal data for one or more specified purposes. Consent must be given in writing, signed by the data subject, and must clearly indicate the data to which it applies, for which purpose and for what period it is given, and who is giving the consent. By signing the consent form, the data subject also confirms to have been informed of his rights in advance. The employee processing the personal data must be able to prove the existence of consent over the entire period of the data processing.
3. An exception to the prohibition under paragraph 1 also applies to the following data:
   a. data concerning the state of health in personal records of employees and students providing that the data were voluntarily provided by the data subject to be kept in records and they are kept for his benefit (e.g., the data affects admission to study, provision of services to special-needs persons, accommodation in dormitories, or calculation of the tax liability or other levies imposed by law);
   b. data concerning membership in trade unions active at the University recorded in personal and wage files of the employees providing that the data were voluntarily provided by the data subject to be kept in records and they are kept for payment of membership fees or other levies, including accounting for such payments;
   c. special category of personal data processed for the purposes of projects/research.
4. Processing which does not require identification of the data subject is governed by Article 11 of the Regulation.

Part Two – Accountability of Persons Ensuring Personal Data Protection

Article 6 – The University

The University is the body accountable for personal data processing under Article 1 (2). It may act both as a controller and a processor. To comply with the requirements of the Regulation and the Act for personal data protection this part of the Directive defines persons participating in ensuring the above stated purpose.

Article 7 – University Level

1. The standing of the Rector arises from the Higher Education Act, the Constitution of the University and other internal regulations of the University. The Rector acts as a governing body of the University responsible for compliance with the principles, rules, and procedures applicable to personal data processing externally as well as internally within the University in cases performed at the central level of the University and in those cases where the powers have not been delegated to other persons stated in this part.
2. Vice-Rectors are accountable to the Rector of the University for compliance with the principles, rules, and procedures applicable to personal data processing performed within their fields of activities and powers stated in Article 11 of the Constitution of the University.
3. The Chief Financial Officer is accountable to the Rector of the University for compliance with the principles, rules, and procedures applicable to personal data processing performed within his powers stated in Article 13 of the Constitution of the University.

Article 8 – Faculties and Other Units

1. The deans of individual faculties of the University are accountable to the Rector for compliance with the principles, rules, and procedures applicable to personal data processing performed by the employees and students of the faculty of the University in the fulfilment of their work or study duties, or by other natural or juridical persons processing personal data based on a contract with the faculty of the University, in the matters they are vested with under section 24 of the Higher Education Act, Articles 15 and 16 of the Constitution of the University, other internal regulations of the University, and Rector’s directives.
2. The directors of other units of the University are accountable to the Rector of the University for compliance with the principles, rules, and procedures applicable to personal data processing performed by the employees of another unit of the University or by students for whom the unit provides instruction in the fulfilment of their work or study duties or by other natural or juridical persons processing personal data based on a contract with the other unit of the University, in the matters they are vested with under Articles 15 and 16 of the Constitution of the University, the rules for the internal governance of the other unit, other internal regulations of the University, and Rector’s directives.
3. The deans of individual faculties of the University and directors of other units of the University appoint no later than within ten days of the date of effect of this Directive a contact person for personal data protection at the faculty or other unit who will cooperate with the data protection officer under Article 13 in performing his tasks under Article 15 concerning personal data processing activities at the given faculty or other unit of the University. The deans of the

faculties and directors of other units inform under part three the data protection officer of the appointment without undue delay.

Article 9 – Accountability of Managers for Personal Data Processing

1. A manager is accountable for compliance with the principles, rules, and procedures (stated in this Directive, in the Regulation, and in the Act) applicable to the processing of personal data performed within the field he is entrusted with, including safe data storage, and manages in this field the processing of personal data performed by employees subordinate to him.
2. A manager carries out in the field he is entrusted with the assessment of the impact of the envisaged processing operations on the protection of personal data under Article 35 of the Regulation. For this purpose, he seeks the advice of the data protection officer under part three.
3. The register of personal data processing activities maintained under part five records, for individual processing activities, the names of the managers in individual faculties or other units of the University within whose powers the given processing falls. In case of doubt concerning the relevant powers, the decision on the competent person for the given processing activity is made by:
   a. the Rector in the case of personal data processing involving the central level of the University;
   b. the dean in the case of personal data processing within the powers of the given faculty;
   c. the director of another unit in the case of personal data processing within the powers of the given other unit;
   d. the Chief Financial Officer in the case of personal data processing within the powers of the Rector's Office which do not involve the central level of the University.
4. For new activities the accountable manager or managers will be determined before commencement of the personal data processing.
5. Persons stated in paragraph 3 inform without undue delay the data protection officer under part three.
6. Managers must ensure that their subordinate employees involved in personal data processing commit themselves to confidentiality. A template of the confidentiality obligation recommended to be included in the employment contracts forms Appendix No. 2 to this Directive.

Article 10 – University Employees

1. The University employees who are involved in personal data processing have a duty to become acquainted with this Directive, the Regulation, other relevant generally binding legal regulations and relevant guidance documents on methodology issued by the data protection officer under Article 15 (1) (j). The manager superior to the employee is responsible for the employee's becoming acquainted with the above documents.
2. Persons stated in paragraph 1 have a duty to process personal data always only within the scope and under conditions determined by the manager who is in charge of the given personal data processing activities.
3. Persons stated in paragraph 1 have a duty to keep the personal data confidential and to keep confidential the security directives the disclosure of which would endanger the personal data security. The confidentiality obligation continues after termination of employment, study, or performance of the relevant work. The scope of the confidentiality obligation is stated in the employment contract.
4. If an employee of the University or other person in an employment relationship with the University, a faculty, or other unit is involved in personal data processing the person is responsible for the personal data processing performed. When processing personal data, the person must follow the instructions and guidance documents on methodology issued by the data protection officer under part three and provide information to the data protection officer as requested.
5. A person in an employment relationship with the University, faculty, or other unit of the University is entitled to raise questions or make suggestions concerning personal data processing and protection to the data protection officer under part three either directly or via a contact person under Article 8 (3).

Article 11 – Students and Lifelong Learning Participants

1. In cases when personal data might be processed in the course of the processing of final theses of students (bachelor's, master's and dissertation theses), participants in rigorosum proceedings and participants in lifelong learning, the thesis advisor or supervisor has a duty to introduce the student, or the participant in rigorosum proceedings or in a lifelong learning programme, to the duties arising from this Directive and the Regulation and to ensure possible further steps in compliance with this Directive.
2. In cases when a teacher of a subject requires that students, or participants in rigorosum proceedings or in a lifelong learning programme, prepare as part of the instruction of the subject an assignment requiring personal data processing, the teacher must introduce the student, or the participant in rigorosum proceedings or in a lifelong learning programme, to the duties arising from this Directive and the Regulation and ensure possible further steps in compliance with this Directive.
3. Further details of personal data processing activities under this Article may be stipulated in a Rector's directive on the advice of the data protection officer.

Article 12 – Other Persons Involved in Personal Data Processing, Processors Acting in a Chain and Processing Contract

1. Where persons without direct legal relationship to the University (e.g., employees of joint workplaces of the University and other institutions, co-researchers of research projects from other institutions, co-authors of publications, etc.) are involved in the processing of personal data for which the University acts as the controller or the processor, it is necessary to introduce such persons to the duties arising from this Directive and the Regulation and the persons must agree to comply with this Directive for example through a contract between the University and the cooperating institution or in other appropriate binding form.
2. The University will make a contract to provide the services of a personal data processor only with persons who will fulfil the role of processor providing sufficient guarantees to implement appropriate technical and organisational directives in such a manner that processing will meet the requirements of legal regulations applicable to personal data processing and ensure the security and protection of personal data as well as the rights and freedoms of data subjects.
3. It is the duty of the employee who negotiates or possibly enters into a contract on behalf of the University, to verify the reliability of the personal data processor and compliance with the requirements for legal personal data processing on the part of the potential processor. A record of the manner of verification and its results is created and inserted in the file of the relevant business case together with the documents used as the basis for verification; the record is also inserted in the file of the relevant personal data processing. The employee under the first sentence also has a duty to provide a notification of the details of the personal data processor using the procedure under Article 20.
4. Previous written consent of the University to processors acting in a chain when the processor provides processing services via third parties may be granted only where it is necessary to fulfil the tasks of the University.
5. Where personal data processing is to be carried out by the University in the role of processor, the personal data processing may involve a partial processor (processors acting in a chain) only providing that the personal data controller agreed to it in the personal data processing contract or granted a written authorisation. The authorisation may be granted either for a person of specific processor, or general where the partial processor is selected by the University within the scope of the authorisation; in such case the controller is entitled to object to the partial processor selected. If the personal data controller objects to the partial processor, it is not possible to involve such partial processor in the personal data processing. If the verification carried out in accordance with paragraphs 2 and 3 reveals that the guarantees in case of a specifically authorised partial processor are not sufficient, the personal data controller is notified of the fact. Such partial processor may be involved in personal data processing only if the personal data controller requests it despite the objections raised by the University. All communication, the documents used as the basis for verification, and the results of verification are inserted in the file of the relevant business case and the file of the relevant personal data processing.
6. Where personal data processing is to be carried out by the University in the role of partial processor within the framework of processors acting in a chain, i.e., as a processor processing personal data for another processor, before entering into the contract the person negotiating the contract on behalf of the University requests the documents proving that the processor was granted authorisation by the personal data controller to involve a partial processor in personal data processing; the documents mean either a specific authorisation to involve the University as partial processor, or a general authorisation to involve a partial processor and a confirmation that the personal data controller raised no objections to the University as partial processor. The documents and related communication are inserted in the file kept for the relevant case and in the file of the relevant personal data processing.
7. A personal data processing contract made between the University and a processor, or possibly between the University and the controller or partial processor, must have the parameters in accordance with Article 28 of the Regulation.

Part Three – Data Protection Officer

Article 13 – Status of the Data Protection Officer

1. The data protection officer (also “the officer”) is directly subordinate to the Rector.
2. The officer is involved in all processes and matters related to protection and processing of personal data at the University.
3. The officer is supported by the University in maintaining his professional knowledge and he is granted access to personal data, processing operations, and to all resources needed for the performance of tasks in Article 15.
4. The University does not give any specific instructions to the officer concerning the fulfilment of his duties. However, the Rector may assign to the officer additional tasks and duties. Such tasks or duties though may not result in a conflict of interest with the execution of his office of data protection officer.
5. The officer is under the duty of confidentiality in relation to the performance of his tasks. The duty of confidentiality continues also after termination of employment.
6. The information on the officer including the contact details is provided at the publicly accessible section of the University website.

Article 14 – Appointment of the Data Protection Officer

The officer is appointed by the Rector based on his professional qualities, in particular expert knowledge and practical experience in the field of personal data protection and the ability to fulfil the tasks listed in Article 15. The Rector may remove the officer from his office.

Article 15 – Tasks of the Data Protection Officer

1. The officer performs in particular the following tasks:

a. provides information and advice to employees and students of the University who carry out the processing of personal data concerning their duties under this Directive, the Regulation and other generally binding legal regulations applicable to personal data protection;
b. monitors compliance with this Directive, the Regulation, other generally binding legal regulations applicable to personal data protection, and with the policies of the University in the field of personal data protection including increasing the awareness and professional training of the staff involved in processing operations;
c. supervises the implementation of personal data protection and processing;
d. provides expert assistance in terms of assessment of the impact on personal data protection and monitors its implementation under Article 35 of the Regulation;
e. after prior consultation with the persons listed in Articles 7 and 8 notifies the cases of personal data breach to the supervisory authority under Article 33 of the Regulation and communicates the cases of personal data breach to the data subject Under Article 34 of the Regulation;
f. cooperates and communicates with the supervisory authority;
g. acts as the contact point for the supervisory authority in matters concerning personal data processing including prior consultation under Article 36 of the Regulation;
h. accepts from the employees of the University submissions to initiate a new personal data processing or to change the existing one and takes views on such submissions;
i. communicates with the data subjects who may contact him in all matters related to the processing of their personal data and exercising of their rights under this Directive and the Regulation;
j. issues guidance documents on methodology concerning personal data processing at the University that are to be followed by persons involved in personal data processing at the University;
k. carries out other tasks arising for his position from the Regulation, the Act, or other generally binding legal regulations, or arising from this Directive and other internal regulations of the University and Rector's directives.

2. The officer supervises the operation of the register of personal data processing of the University stated in Article 19.
3. When performing his tasks, the officer bears in mind the risk related to processing activities and at the same time takes into account the nature, scope, context, and purposes of the processing.

Article 16 – The Powers of the Data Protection Officer at the University

1. If the officer finds out that there is a danger of breach of the rules for the protection of personal data arising from the Regulation, the Act, or this Directive, or if a breach occurs, the officer has a duty to inform the managers thereof under Article 9 and recommend in writing the removal of the defective or risky condition. Under Article 9, a manager has a duty to discuss the condition with the officer within a reasonable time, and if he agrees with the findings of the officer, he must refrain from further defective or risky conduct. The manager also has the duty, under Article 9, to adopt all directives to ensure that the situation does not occur again.
2. If a manager, under Article 9, does not agree with the recommendation of the officer, he communicates this in writing to the officer and states the reasons why he believes that no breach of rules stated in the first sentence of paragraph 1 occurred or that there is no danger that such breach may occur. In such case the officer communicates this fact to persons competent in the relevant subject matter listed in Articles 7 and 8 and refers to them the entire file of documents.
3. The officer has a duty to suggest that general or specific directives in the field of personal data protection be adopted to persons stated in Articles 7 and 8 whenever:
   a. based on his findings under paragraph 1, he concludes that there is a danger of breach of rules or a breach occurred;
   b. it is appropriate further to the general application practice in the field of personal data protection.
4. The provisions of paragraphs 1 and 4 are not to the prejudice of the officer's duty to notify, after prior consultation with the persons listed in Articles 7 and 8, cases of personal data breach to the supervisory authority and to communicate them to the data subject under Article 15 (1) (e).

Part Four – Data Subject

Article 17 – Data Subject

A data subject is a natural person whose personal data are processed. During personal data processing activities at the University the data of the following data subjects are processed:

a. employee of the University (or a person in an employment relationship with the University);
b. job applicant;
c. applicant for admission to study;
d. student of the University;
e. former student of the University (including graduates);
f. a participant in a lifelong learning programme;
g. a student of another higher education institution or a student on a short-term study stay at the University;
h. a business partner (supplier, purchaser, customer);
i. a participant in research;
j. external collaborator (e.g., supervisor, co-researcher, co-author of a publication);
k. a visitor or participant in an event organised by the University;

l. a participant in administrative or judicial proceedings with the University;
m. another person.

Article 18 – Information Provided to Data Subject

1. The University in the role of controller provides information to a data subject pursuant to Article 12 of the Regulation in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.
2. Where personal data are collected from the data subject, the controller provides, at the time when personal data are obtained, the data subject with all the following information:
   a. contact details of the University;
   b. contact details of the data protection officer;
   c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
   d. where the processing is based on Article 4 (1) (f), the legitimate interests pursued by the University or by a third party;
   e. the recipients or categories of recipients of the personal data, if any;
   f. where applicable, the fact that the University intends to transfer personal data to a third country (i.e., to a country that is not a member of the European Union) or international organisation and reference to the appropriate safeguards and the means by which to obtain a copy of them or where they have been made available.
3. In addition to the information referred to in paragraph 2, the University provides the data subject with further information stated in Article 13 (2) of the Regulation necessary to ensure fair and transparent processing.
4. Where personal data have not been obtained from the data subject, the controller provides the data subject with the following information:
   a. contact details of the University;
   b. contact details of the data protection officer;
   c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
   d. the categories of personal data concerned;
   e. the recipients or categories of recipients of the personal data, if any;
   f. where applicable, the fact that the University intends to transfer personal data to a third country (i.e., to a country that is not a member of the European Union) or international organisation and reference to the appropriate safeguards and the means by which to obtain a copy of them or where they have been made available.
5. In addition to the information referred to in paragraph 4, the University provides the data subject with further information stated in Article 14 (2) of the Regulation necessary to ensure fair and transparent processing.
6. The University in the role of controller makes all communications pursuant to Articles 15 to 22 and 34 of the Regulation.
7. Information under this article is provided in electronic form on the website of the University and in the information systems of the University, or in other appropriate provable form.

Article 19 – Rights of Data Subject

1. The rights of the data subject form an integral part of the personal data protection at the time of processing.
2. Above all, the data subject has a right:
   a. to access to personal data pursuant to Article 15 of the Regulation;
   b. to be informed of the personal data processing;
   c. to rectification pursuant to Articles 16 and 19 of the Regulation;
   d. to erasure pursuant to Articles 17 and 19 of the Regulation;
   e. to restriction of processing pursuant to Articles 18 and 19 of the Regulation;
   f. to data portability pursuant to Article 20 of the Regulation;
   g. to object pursuant to Article 21 of the Regulation;
   h. automated individual decision-making governed by Article 22 of the Regulation.
3. Data subjects may contact the data protection officer in all matters related to the processing of their personal data and exercise of their rights under this Directive and the Regulation.
4. All communications to the data subjects including information on their rights and notification in the case of the exercise of rights of the data subject are provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, where among other things the age of the recipient of information is taken into account. To ensure the intelligibility of the information provided, multi-layered information is used where appropriate.
5. A record is created of compliance with the information duty, exercise of rights of data subjects, and handling of exercise of rights of data subjects including refusal of a request by a data subject, etc. The record includes the documents used as a basis by the responsible person including the request/letter through which the data subject exercised the right. Unless explicitly stated otherwise, the record is inserted in the file of the relevant personal data processing and archived for a period reflecting the limitation periods and lapse periods of civil and public delicts that may be committed in relation to personal data processing.
6. Where the data subject exercises his rights, in order to protect the rights and legally protected interests it is necessary to verify in an appropriate form the identity of the data subject who requests access and the data subject has a duty to provide sufficient proof of identity. It is considered sufficient proof of identity when the application is sent by email

with an electronic signature, via data box or by means of a postal service operator where the document is signed and the authenticity of the signature of the acting person is officially verified and the application includes the identification details in the scope required by section 14 (2) of Act No. 106/1999 Sb. to regulate free access to information.

7. The data protection officer provides to the data subject upon his request under Articles 15 to 22 of the Regulation information on adopted directives without undue delay and in any case no later than within one month of receiving the application. This time limit may be extended by two more months if required due to the complexity and number of applications. The officer informs the data subject on any such extension including the reasons for the delay within one month of receiving the application. If the data subject submits the application in electronic form, then the information is provided in electronic form if possible, unless the data subject requests that the information be provided in another form.

Part Five – Register of Personal Data Processing Activities

Article 20 – Registration and Recording of Personal Data Processing Activities

1. An electronic register of personal data processing activities at the University ("the register") is created to provide an overview of personal data processing at the University. The Information Technology Institute of the University ("the institute") is authorised to operate the register. The director of the institute is responsible for the operation of the register.
2. Faculties and other units of the University processing or intending to process personal data subject to this Directive or wanting to change the current mode of personal data processing must notify the data protection officer of this fact via the email address gdpr@cuni.cz.
3. The notification pursuant to paragraph 2 must contain a complete characteristic of the relevant personal data processing in the following scope:
   a. name of the agenda, or processing activity;
   b. description of the processing activity;
   c. types of data subjects pursuant to Article 17 whose data are processed by the activity;
   d. list of personal data or groups of the data that are processed by the activity;
   e. types of documents that are processed by the activity;
   f. information on the transfer of personal data outside the University;
   g. location of the processed personal data and identification of the information system or application, if used in the processing activity;
   h. information on when and how the personal data are or will be removed from the agenda;
   i. the roles involved in the processing activity;
   j. managers accountable for the processing activity pursuant to Article 9;
   k. the legal basis and purpose of the processing activity;
   l. information on processors, if they are involved in the agenda, including the scope of data made available to them and the processing they carry out;
   m. general description of the technical and organisational security directives to secure the personal data that are appropriate to the risks to the rights and freedoms of data subjects pursuant to Article 32 (1) of the Regulation.
4. The person submitting notification is entitled to commence new or change the existing personal data processing only after receiving the consent issued by the data protection officer based on the notification pursuant to paragraph 3 and the subsequent assessment of the personal data processing activity and its protection. In case the data protection officer fails to give consent, further steps are consulted with persons listed in Articles 7 and 8.
5. The data protection officer or a person designated by him enters the information on the new personal data processing activity or on changes to existing personal data processing activity in the register based on the details pursuant to paragraph 3 above after the data protection officer expressed his consent to the processing or change of personal data processing pursuant to paragraph 4.

Part Six – Making Personal Data Public and Disclosing them to Third Parties

Article 21 – Making Personal Data Public

1. Making personal data public means giving access to the data to persons or groups of persons not specifically identified, in particular by means of mass media, other public communication, or as part of a public list (e.g., in the publicly accessible section of the University website).
2. A student may, after logging into the information system of the University ("the system"), change the setting so that an anonymous user may retrieve his personal data.
3. If retrieving a student's personal data is enabled, the following data of the student will be displayed:
   a. surname and name (or surname and names);
   b. degrees;
   c. faculty;
   d. programme of study, field of study, specialisation, if any;
   e. year of study; and

f. in case of completed study the academic year of completion.

4. A student may, after logging into the system, set up which other data about him should be made public.
5. An anonymous user of the system or a logged-in user other than a University employee or teacher ("an anonymous user") cannot retrieve the student's data based on entered criteria unless the student whose data the anonymous user intends to retrieve enabled such search using the procedure pursuant to paragraph 2.
6. A person who studied at the University and has completed his studies may enable the retrieval of his data using one of the following ways:
   a. if he knows his log-in data for the system he may log into the system and enable the retrieval of his data directly in the settings of the system;
   b. he may request a change in the settings via email to the address helpdesk@is.cuni.cz or via the data protection officer.
7. The data of persons who studied at the University and have completed their studies are not retrievable for an anonymous user unless such persons enabled the retrieval using the procedure described in paragraph 6; this provision is without prejudice to the provision of paragraph 8.
8. With regard to the publishing of final theses under section 47b of the Higher Education Act in the case of persons who defended a final thesis after 1 January 2006, the following data are made public:
   a. surname and name (or surname and names);
   b. degrees;
   c. date of birth;
   d. faculty;
   e. programme of study, field of study, specialisation, if any;
   f. the name of the department which published the topic of the thesis;
   g. type of thesis (bachelor's, diploma, rigorosum, dissertation);
   h. title of the thesis;
   i. full text of the thesis including appendices;
   j. language of the thesis;
   k. key words of the thesis;
   l. abstract;
   m. thesis advisor;
   n. consultant;
   o. reviewers of the thesis;
   p. report of the thesis advisor;
   q. report of the reviewer or reviewers;
   r. date of defence;
   s. record of the course of defence;
   t. result of defence (grade).
9. If a student is currently a member of self-governing academic bodies or advisory bodies of the University, the data pursuant to paragraph 11 a), b), c), h), i), and j) are made public concerning such student and he may enable the publishing of other data under paragraph 13. If a student is involved in teaching, the data pursuant to paragraph 11 a), b), c), f), i), j), k), l), m), n), and o) are made public concerning such student. If a student is involved in creative activities of the University, the data pursuant to paragraph 11 a), b), c), f), m), and n) are made public concerning such student.
10. The data of applicants for admission to study are not made public, an anonymous user is not able to retrieve data of the applicants for admission to study.
11. The University publishes by means of its website the outputs from the system containing the following data of employees and basic data of their employment:
   a. name;
   b. surname;
   c. degrees;
   d. type of employment (employment contract, agreement to perform work, agreement to complete a job);
   e. faculty or other unit of the University where the person is employed;
   f. the workplace, i.e., an organisational unit or units of faculty or of another unit of the University, where the work is performed;
   g. position (full professor, associate professor, assistant professor, assistant, lecturer, etc.);
   h. offices at the workplace and in the bodies of the University, faculties, and other units;
   i. contact details in relation to the University (addresses of workplaces, location of office, telephone and fax numbers, email addresses);
   j. the subject area or other specialisation of the employee;
   k. office hours;
   l. the course of academic qualifications;
   m. the share of individual types of creative activities of the University;
   n. information on publications;
   o. instruction implemented at the University.

12. The data pursuant to paragraph 11 are made public on a mandatory basis for employees with a valid employment contract. The same data are made public on a mandatory basis for employees working on the basis of an agreement to perform work, unless the superior of such employee decides otherwise. The data on an employee and his employment relationship are not made public for employees working on the basis an agreement to complete a job, unless the employee's superior decides otherwise.
13. Additionally, the employee has the right to enable publishing and to choose its specific scope for the following data:
    a. photograph;
    b. curriculum vitae;
    c. personal website related to the employee's activities at the University;
    d. other data published by the employee himself, if any.
14. In the case of joint workplaces of the University and other institutions (primarily the university hospitals and institutes of the Czech Academy of Sciences), the University also publishes the data of the employees of such other institutions if they are involved in the activities of the University in the scope under paragraph 11 a), b), c), and f) to o).
15. A participant in lifelong learning may, after logging into the system, enable the retrieval of his data by an anonymous user.
16. If retrieval of data of a participant in lifelong learning is enabled, the following data are displayed:
    a. surname and name (or surname and names);
    b. degrees;
    c. faculty or other unit of the University;
    d. lifelong learning programme;
    e. year of study;
    f. in case of completed study in lifelong learning programmes, the academic year of completion.
17. A participant in a lifelong learning programme may, after logging into the system, set up which of his data should be displayed.
18. An anonymous user of the information system cannot retrieve the data on a participant in a lifelong learning programme based on entered criteria unless the participant whose data the anonymous user intends to retrieve enabled such search using the procedure pursuant to paragraph 15.
19. A participant in a lifelong learning programme who studied at the University and has completed his studies in the lifelong learning programme may enable the retrieval of his data using one of the following ways:
    a. if he knows his log-in data for the system he may log into the system and enable retrieval of his data directly in the settings of the system;
    b. he may request a change in the settings via email address helpdesk@is.cuni.cz or via the data protection officer.
20. In case of academic officials and persons who are currently members of self-governing academic bodies or advisory bodies of the University who are not in an employment relationship to the University, the data pursuant to paragraph 11 a), b), c), h), and i) are made public.

Article 22 – Disclosing Personal Data to Third Parties

1. The disclosure of personal data to third parties other than the University is governed by this Directive, the Regulation, and the generally binding legal regulations in force.
2. Every disclosure of personal data to a third party other than the University must be recorded in the register, including the scope of provided data, purpose of disclosure, and identification of the third party.
3. The managers for the given activities or fields of processing pursuant to Article 9 are accountable for compliance with the correct procedure for disclosure of personal data to third parties other than the University in accordance with this Directive, the Regulation, and the generally binding legal regulations in force.

Article 23 – Personal Data Security

1. Documents and mobile/external/portable technical data carriers that are at the disposal of the University and that contain personal data protected under this Directive must be kept only in lockable cabinets or in rooms designed for this purpose in the workplaces of the University, or where applicable, in other secure places depending on the characteristics of the relevant data processing, or they must be secured by encryption. Only copies of these documents or carriers may be taken out of a workplace of the University under conditions stipulated in paragraph 3. In the case of online transfer of data outside of the University, the personal data transferred must be encrypted and must be protected in an appropriate way pursuant to the Regulation and ensured by a contract with the recipient or the processor of the transferred data. The essential elements of the contract with the processor are stated in Appendix No. 1 to this Directive.
2. Computers and other technical means on which data are stored containing personal data protected under this Directive must be secured against free access by unauthorised persons, usually by passwords, encryption, or locking. Data stored on such technical means that are not related to the activities of the University (e.g., personal files of Employees and students of the University) are not subject to this directive.
3. Copies of personal data protected pursuant to this Directive must be made on technical data carriers in compliance with the operating rules stipulated for individual data processing activities and stored in lockable cabinets at the workplaces of the University or where applicable, at other secure places depending on the characteristics of the relevant data processing or they must be secured by encryption. If these copies are carried away from the premises of

the University, additional safety directives must be taken (locking, encryption, etc.) to prevent both accidental access to the data by an unauthorised person and intentional unauthorised attempt to access the data.

4. If an employee or a student of the University finds out or suspects that a personal data breach might occur or has occurred he has a duty to immediately notify the data protection officer and the persons stated in Articles 7 and 8.
5. Notification of cases of personal data breach to the supervisory authority under Article 33 of the regulation and communication of the personal data breach to the data subject under Article 34 of the Regulation is carried out by the data protection officer after prior consultation with the persons listed in Articles 7 and 8.

Part Seven – Transitional and Final Provisions

Article 24 – Transitional and Final Provisions

1. Rector's Directive No. 28/2015 regulating processing of personal data of students, applicants for admission to study, employees and other persons at Charles University is hereby repealed.
2. In cases of existing personal data processing activities the powers of the managers under Article 9 will be determined no later than within ten days of the date of effect of this Directive.
3. The data protection officer under Article 15 (1) is authorised to interpret individual provisions of this directive.
4. An audit of compliance with this Directive is performed by the data protection officer under Article 15 (1).
5. This directive becomes effective on 25 May 2018

.

Appendices:
Appendix No. 1 – Essential elements of the contract on personal data processing
Appendix No. 2 – Confidentiality obligation of employees

In Prague on 27 April 2018

Prof. MUDr. Tomáš Zima, DrSc., MBA
Rector

Appendix No. 1 to Rector's Directive No. 16/2018 – - Principles and Rules of Personal Data Protection

Essential elements of personal data processing contract

A full list of essential elements of every contract between a controller and a processor is provided in Article 28, in particular in paragraphs 2 and 3, of the General Data Protection Regulation and in section 32 of the new act on the protection of personal data that is in preparation.
The contract with the processor must always clearly set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and all the obligations and rights of the controller and the processor.
The subject matter of the processing may be identical with the subject matter of the contract, for example: "The subject matter of the contract consists in processing of the below stated personal data."
The duration of the processing should always be identical to the duration of the contract because after termination of the contract the processor returns the data to the controller or is obliged to erase the data.
The nature of personal data processing means how the data are processed, whether in writing or electronically. This applies not only to the processing itself but also to obtaining the data from the data subjects.
The purpose of the processing means a specific description of our need, that is for example to ensure employment relations, maintain the register of students, produce and hand over the students'/employees' identity cards, or to process a medical report of a patient.
The type of personal data means the specific identification of the data, such as the name, surname, the date of birth, birth certificate number, identity card/passport number, residence, contact details, gender, diseases, etc.
The category of data subject means whether the person is an adult or a child, employee, or student, patient, or a third party, a contractor, etc.
The rights and obligations of the controller and the processor may be broadly defined, but in any case the contract should contain at least clauses similar to those listed below:

- "The processor is not allowed to transfer without the previous written consent of the controller any part of his obligations arising from this contract to a third party (another processor). If all of the obligations or a part of the obligations of the processor are transferred with previous written consent of the controller to a third party, the processor shall be liable for any damage caused by the third party to the extent of his own liability, as if the damage was caused by himself, without any limitation."
- If the prior consent of the data subject is required for the processing of personal data, this fact must be stated in the contract: "The controller/processor agrees to obtain prior written consent to the processing of personal data under this contract from individual data subjects whose personal data will be processed under this contract."
- "The processor agrees to take all security, technical, and organisational directives to protect the personal data and other directives required in Article 32 of the Regulation; in particular the processor agrees to take all directives to prevent unauthorised or accidental access to personal data, alteration, destruction or loss of the data as well as abuse of the data including directives related to the operation of information systems in which the personal data are processed."

- The processor further agrees:
  a. not to use personal data for a purpose other than that stated in this contract and to process the personal data only on documented instructions from the controller with the exception of the cases when this duty is imposed on the processor directly by a legal regulation;
  b. to take with due professional care all control and protective directive to protect the personal data and to enable controls, audits, or inspections carried out by the controller or by another competent body under legal regulations;
  c. to comply with all control and protective directives to protect the personal data with due professional care;
  d. to provide to the controller without undue delay or within a time limit set by the controller the cooperation required for the discharge of the legal duties of controller related to personal data protection, the processing thereof, and the discharge of the personal data processing contract;
  e. to inform the controller of all facts having an impact on personal data processing;
  f. to notify the controller of any doubts concerning compliance with the law or a personal data breach;
  g. if required, to provide to the controller all support and assistance in contact and negotiations with the Office for Personal Data Protection and with data subjects;
  h. to react without undue delay to the requests of data subjects, to inform them of all their rights and to provide access to processing information upon request;
  i. after the termination of the provision of services related to processing, to duly handle the processed personal data in accordance with the needs of the controller, i.e., either erase all personal data or return them to the controller based on the controller's instructions;
  j. to comply with all other duties imposed by legal regulations even if they are not explicitly stated in the contract;
  k. to make all possible efforts to eliminate any unlawful state in relation to transferred personal data under this contract that would result in a breach of duties by acts of the relevant contracting party, immediately after such state has occurred.
- Any information containing personal data exchanged by the contracting parties during implementation of this contract is confidential. The processor agrees not to disclose the information to a third party and not to use the information contrary to the purpose for which it was provided (i.e., the purpose of discharge of this contract), unless explicitly stipulated otherwise in this contract. The processor agrees not to disclose information related to this contract to any other person and not to use the information for any purpose other than that stipulated in this contract over the term of this contract as well as after its termination (except for cases when he has a duty to do so under a legal regulation or when both contracting parties agree thereon in writing). The processor must make sure that the persons authorised to process personal data commit themselves to confidentiality or that they be subject to the legal duty of confidentiality."

It is recommended that contractual penalty for breach of the above duties and obligations of the processor be stipulated and in the case of a repeated breach on the part of the processor the contract should also stipulate the right to immediately withdraw unilaterally from the contract.

The contract should also state that all documents related to personal data processing including those provided by the controller to the processor and those created by the processor, must be stored and archived at a secure location at the following address ….. (fill in an address that is as close to the processor as possible, however it must be in the Czech Republic).

If the processor is a foreign person, it is recommended that the contract contain the following clause: "All documents and communication related to personal data processing and to ensuring the activities under the contract shall be in Czech language and any disputes shall be resolved in accordance with Czech law before a court having territorial and subject-matter jurisdiction over the controller based on the controller's registered office. Arbitration is excluded."

Even if the contract is made for a fixed term it is advisable to include the possibility to terminate the contract before the term expires for the case when the processor makes mistakes which do not entitle the controller to withdraw from the contract, however it is prudent to terminate the contract, or where applicable it may be economically advantageous for Charles University because other better processors may be available. As the period of notice of termination of the contract should be reciprocal, the period of notice should be stipulated so that it does not endanger Charles University in case of termination of the contract by the processor.

Appendix No. 2 to Rector's Directive No. 16/2018 - Principles and Rules of Personal Data Protection

Recommended wording of the duty of confidentiality to be included in employment contracts at the University

"The employee agrees not to disclose information and facts obtained during employment that are identified by the employer as confidential under section 276 (3) of Act No. 262/2006 Sb., the Labour Code, as amended ("the Labour Code"), or subject to trade secret under section 504 of Act No. 89/2012 Sb., the Civil Code, as amended, or that are not made public or intended for publication by the employer.

The employee further agrees not to disclose personal data obtained during employment the disclosure of which would jeopardise the security of such personal data in accordance with section 47 of Act No. 110/2019 Coll. on personal data processing, as amended. The employee notes that this duty of confidentiality is not extinguished by the termination of employment.

The employee further notes that breach of these obligations may be deemed a breach of the employee's obligations under section 301 (d) of the Labour Code. In case of damage arising in relation to breach of the duty of confidentiality the employee is liable for the damage to the employer in accordance with section 250 (1) of the Labour Code."

download