Privacy and Disclosure Policy

Effective date: 11 July 2023

Book I - Privacy Policy

Table of contents

Preamble

the Semmelweis University hereinafter: University) under Act CCIV of 2011 on National Higher Education (hereinafter: Nftv.), Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: Infotv.), Act CLIV of 1997 on Health Care (hereinafter: Eütv.), Act XLVII of 1997 on the processing and protection of personal data concerning health and related personal data (hereinafter: Eüak.) and 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 Regulation (EC) No 95/46/EC (hereinafter: Regulation), it establishes the following rules for data management at the University.
The Privacy Policy (hereinafter: Policy) shall be interpreted and applied in accordance with the provisions of the Regulation. To promote uniform interpretation and application, the Centre for Privacy and Patient Rights (hereinafter: ABK) provides support.

1. GENERAL PROVISIONS

1.1. Purpose of the Policy

To define the rules governing the processing activities carried out by the University as a data controller.

1.2. Scope of the Policy

(1) The scope of the Policy extends to the following:
   a) all data classified as personal by the applicable legislation;
   b) the University and all its departments where personal data is processed;
   c) to anyone who processes personal data or becomes aware of personal data in the course of their activities at the University.

(2) The scope of this Policy does not extend to institutions maintained by the University, business entities owned by the University, any entity with legal personality that is a participant in or related to the operation of the University (hereinafter referred to as "entities"), but the University, as the maintainer, owner or participating member of such entities, encourages and expects such entities to develop their own data protection systems in accordance with this Policy.

1.3. Applicable legislation, definitions, forms

(1) The terms used in these rules correspond to the terms defined in the legislation in force.
(2) For the purposes of the Policy:
   a) Organizational unit obliged to appoint a local data protection officer: the organizational unit classified as Level I in the register of organizational units of the University's Organizational and Operational Rules, the patient care organizational unit (clinics and the Pető András Rehabilitation and Health Care Department), the University Student

Self-Government and the Doctoral Student Self-Government among the other organizations classified as Level I.

(3) The use of the forms published in the forms library - with the specified data content - is mandatory.

1.4. Principles, legal basis and purposes of data processing

(1) The University shall carry out its data management activities in accordance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation and limited retention, accuracy and the principles of integrity and confidentiality, as set out in Article 5 Section (1) of the Regulation.

(2) The University shall implement appropriate technical and organisational measures to ensure that the University's processing of data is carried out in accordance with the principle of data protection by design and by default, as set out in Article 25 of the Regulation.

(3) All departments of the University will ensure that the University is able to demonstrate compliance with the principles and rules of data management (accountability principle).

(4) In the case of an activity involving the processing of personal data, the department concerned shall exercise the tasks incumbent on the controller in accordance with the guidelines laid down by the DPO.

(5) The University will only process personal data if

a) the data subject has given their consent to the processing of their personal data for a specified purpose;

b) [1]processing is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into the contract;

c) [2]processing is necessary for compliance with a legal obligation to which the controller is subject;

d) [3]processing is necessary for the protection of the vital interests of the data subject or of another natural person;

e) [4]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) [5]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 the protection of personal data, in particular where the data subject is a child.

(6) Special data can be processed if

[1] REGULATION Article 6 (1) b)
[2]REGULATION Article 6 (1) c)
[3]REGULATION Article 6 (1) d)
[4]REGULATION Article 6 (1) e)
[5]REGULATION Article 6 (1) f)

a) [6]the data subject has given their explicit consent to the processing of the special categories of personal data for one or more specified purposes, unless Union or Member State law provides that the general prohibition on processing special categories of personal data cannot be lifted by the data subject's consent;

b) [7]processing is necessary for the purposes of complying with the obligations of the controller or the data subject arising from legal provisions governing employment, social security and social protection and for the exercise of their specific rights, where such processing is permitted by Union or Member State law, including Union or Member State law providing adequate safeguards to protect the fundamental rights and interests of the data subject, or by collective agreements under national law;

c) [8]processing is necessary for the protection of the vital interests of the data subject or of another natural person where the data subject is physically or legally incapacitated and is unable to give their consent;

d) [9]the processing is carried out in the context of the legitimate activities of a political, philosophical, religious, trade-union or other non-profit foundation, association or any other non-profit organisation, with appropriate safeguards, on condition that the processing relates solely to current or former members of such an organisation or to persons who have a regular contact with the organisation in relation to the purposes of the organisation and that the personal data are not disclosed to persons outside the organisation without the consent of the data subjects;

e) [10]processing for preventive health or occupational health purposes, to assess an employee's fitness for work, to make a medical diagnosis, to provide health or social care or treatment, or to manage health or social care systems and services, as required by EU or Member State law or under a contract with a health professional;

f) [11]the processing is necessary for reasons of public interest in the area of public health, such as the protection against serious cross-border threats to health or to ensure a high level of quality and safety of healthcare, medicines and medical devices, and is based on Union or Member State law which provides for adequate and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

g) [12]the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of Union or Member State law which is proportionate to the aim pursued, respects the essential content of the right to the protection of personal data and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject.

[6]REGULATION Article 9 (2) a)
[7]REGULATION Article 9 (2) b)
[8]REGULATION Article 9 (2) c)
[9]REGULATION Article 9 (2) d)
[10]REGULATION Article 9 (2) h)
[11]REGULATION Article 9 (2) i)
[12]REGULATION Article 9 (2) j)

(7) [13]The data subject shall be informed before the data are collected of the information on the basis of which the processing is carried out with regard to Articles 13 and 14 of the Regulation. This takes the form of the publication of a privacy notice.

(8) [14]On the basis of consent, where the data subject gives their freely given, explicit, informed and unambiguous consent to the processing of personal data concerning him or her.

a) Consent covers all processing activities carried out for the same purpose or purposes.
b) In the case of processing for multiple purposes, consent must be given for each of the purposes for which the data are processed.
c) With consent, processing may only be carried out in a way that is in compliance with the requirements of prior information and is of a voluntary nature. Voluntariness cannot be justified if the data subjects have given their consent to the processing of data solely in the interests of the University in a subordinate relationship, in bulk, in a specific group of persons, without exception.
d) Consent may be given in any form in which the data subject can be identified and the fact of consent is recorded,
e) consent cannot be given orally, by telephone
f) consent may be given in particular to the following:
   fa) in writing (signed by the person concerned);
   fb) electronically, following the individual identification of the data subject (e.g. identification with the study system), if the fact of consent is recorded (logged);
   fc) by electronic means from an electronic mail address registered by the University concerned, provided that the message is recorded and preserved without alteration.

(9) The local data protection officer shall keep a record of the consents given by the data subjects, with the following content:

a) the name and file number of the processing register,
b) the registration number of the consent to processing,
c) the natural person identification data of the data subject,
d) the date on which consent was given,
e) the registration number of the privacy notice,
f) the date of withdrawal of consent.

(10) [15] Pursuant to Article 8 (4) of Act I of 2012 on the Labour Code, the Eütv and the Eüak, as well as other rules requiring confidentiality, employees who handle data at the University's organisational units are obliged to keep personal data obtained in the course of their activities confidential without any time limit. Confidentiality does not extend to the statutory obligations to provide information, complaints and notifications of public interest, as well as to the disclosure of data of public interest and to the obligation to provide information and notifications of public interest.

(11) [16]A new employee of the University will receive basic data protection information as part of their induction package when they start work. Further training and education will be

[13]REGULATION Article 12 (1)
[14]REGULATION Article 7
[15]2012. Act No.: I Article 8 (4), Article 25 of Act CLIV of 1997 on Health Care and Article 219 of Act C of 2012 on the Criminal Code
[16]REGULATION Article 39 (1) b)

organised by the ABK. The local data protection officer keeps records of employee training, including the following:

a) the name of the participant in the training,
b) the date of the basic training,
c) further training date.

1.5. Data protection by design, data protection impact assessment

(1) [17]At the request of the Local Data Protection Officer, the ABK will carry out an impact assessment of the personal data protection implications of the envisaged processing operation before starting new processing operations (in particular when new processing technologies are used), if they are likely to present a high risk to the rights and freedoms of natural persons.

(2) The DPO must seek the professional advice of the DPO when carrying out a data protection impact assessment.

(3) An impact assessment should be carried out in the following cases:
   a) when carrying out a systematic and extensive assessment of certain personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions which produce legal effects concerning a natural person or similarly significantly affect a natural person are based,
   b) large-scale systematic surveillance of public places, such as the use of an electronic surveillance system (camera) that meets these conditions;
   c) for processing of a large number of health and other sensitive data; for processing that is on the supervisory authority's list of mandatory data protection impact assessments.
   d) If the data protection impact assessment concludes that the envisaged processing would in fact present a high risk in the absence of measures to mitigate the risks, the DPO consults the supervisory authority before processing personal data.

(4) The University will ensure that its internal policies, work instructions and contracts comply with data protection requirements. Before issuing regulations, instructions, (internal regulatory documents), work instructions, model contracts, the opinion of the ABK shall be sought on matters relating to the processing of personal data. When authorising regulations and instructions, the authorisation of the Regulation shall be indicated where relevant.

1.6. Enforcing data protection principles and ensuring accountability

(1) [18]The University may process personal data if:
   a) The processing is required by law (mandatory processing). Such processing includes in particular processing in connection with higher education activities, employment, public education activities or the provision of health services.

[17]REGULATION Articles 25 and 35
[18] REGULATION Articles 5 (2), 5 (1) and Article 6

b) The processing is necessary for compliance with a legal obligation. In particular, such processing is processing that is strictly necessary for the fulfilment of a legal obligation (e.g. providing data).
c) The data subject shall consent to the processing in accordance with 1.4. (8) a) to c). Such processing includes, in particular, processing related to the sending of newsletters based on voluntary subscriptions, participation in events, prize draws, the completion of questionnaires or participation in scientific research.
d) Processing is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into the contract; Such processing may, in particular, take place in the course of a voluntary service provided by the University.
e) Processing is necessary for the protection of the vital interests of the data subject or of another natural person;
f) The processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

(2) [19]The University will take the following measures to ensure that the principles of data management are applied when processing personal data:
a) [20]For legality, fairness and transparency: The processing of personal data must be lawful, fair and transparent for the data subject. When processing personal data, natural persons should be given transparency about the legal basis, the way and means of collecting and using their personal data, the scope of the data processed and the possibility and means of accessing them. In order to ensure that the processing of personal data is transparent to the data subject, the local data protection officer shall keep a register of all processing for each processing purpose, and shall draw up a processing notice for each processing operation recorded therein, which shall be registered and made publicly and unrestrictedly available on the website of their department.
b) [21]Goal orientation: Personal data may only be collected for specified, explicit and legitimate purposes. Personal data may not be processed in a way incompatible with these purposes.
c) [22]Data economy: Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
d) [23]Accuracy: Personal data must be accurate and up-to-date, i.e. all reasonable steps must be taken to ensure that personal data which are inaccurate for the purposes for which they are processed are erased or rectified without undue delay.
e) [24]Limited storability: Personal data must be kept in a form which permits identification

[19] REGULATION Articles 5 (2), 5 (1) and Article 6
[20]REGULATION Article 5 (1) a)
[21]REGULATION Article 5 (1) b)
[22]REGULATION Article 5 (1) c)
[23]REGULATION Article 5 (1) d)
[24]REGULATION Article 5 (1) e)

of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept for longer periods only if there is a legitimate need to process the personal data thereafter. In order to ensure that the storage of personal data is limited to the necessary period, the University sets a time limit for the deletion of personal data for all its processing in its data management policy and records this time limit in its data management records.

f) Integrity and confidentiality: Personal data must be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by implementing appropriate technical and organisational measures.

g) [25]Accountability: the ABK will provide practical assistance to ensure compliance with the requirements of this policy in the design of the processes involved in data management. The DPO reviews compliance with data protection requirements on an annual basis, and the DPC reviews compliance on a case-by-case basis throughout the year. The ABK regularly verifies the current state of compliance through annual self-audit reports prepared by the local data protection officers.

1.7. Data management and security standards in the course of administration

(1) [26]The University employee shall keep documents containing data that are considered personal data under the provisions of the Infotv., the Regulation and these Regulations in a locked cabinet outside working hours and, if possible, during working hours. Official documents may be stored on the desk and other places in the office only for the purpose and duration of work.

(2) [27]A document containing personal data held by the administrator or in the archives may be inspected by a person other than the administrator and the head of the administrator only if the law so permits or if the administrator certifies in a request that the performance of their duties so requires.

(3) [28]In the absence of a legal authorisation, data may only be transferred to a third party with the consent of the data subject. Where the data subject does not consent to the transfer of their data to another body, he or she must be informed that their request cannot be met or cannot be met in full.

(4) When transferring data within the university, the data requester is always required to justify the purpose and legal basis of the data request. The transfer of data can only take place after this has been verified.

(5) [29]In exercising the right of access, the data subject or their representative must act in a way that does not violate the rights of others (personal or proprietary data relating to another person must be hidden or otherwise made unidentifiable). The same procedure should be followed when making a copy or extract.

[25]REGULATION Article 5 (2)
[26]REGULATION Article 5 (1) f)
[27]REGULATION Article 5 (1) f)
[28]REGULATION Article 6 (1)
[29]REGULATION Article 5 (1) f)

(6) [30]The administrator who holds the documents listed in paragraph 1 at the end of working hours shall be responsible for their safekeeping. In addition to other considerations, for data protection reasons, premises where shared printers or copiers are in operation should be used in accordance with data security requirements.

(7) [31]In addition to other considerations, for data protection reasons, premises where shared printers or copiers are in operation should be used in accordance with data security requirements. The administrator shall manage and store the computer and the data media used in connection with it in such a way that the data requiring protection cannot be accessed by unauthorised persons. They are also obliged to switch off the workstation at the end of working hours, except for workstations that are kept permanently on and online, and to lock the door.

(8) [32]Documents containing personal data may be removed from the University premises, except for the performance of official duties, only with the permission of the immediate superior. The administrator must ensure that it is not lost, damaged or destroyed and that its contents are not disclosed to any unauthorised person.

(9) [33]The data are no longer necessary for the purposes for which they were processed and data for which the purposes for which they were processed have ceased or have been modified shall be destroyed without undue delay or after the expiry of the retention period provided for in the Data Management Policy. Other documents containing personal data must also be destroyed with the necessary security measures.

(10) [34]The head of the department shall define the access rights to individual records and data management by person and job function in accordance with the provisions of the Information Security Policy.

(11) [35]In proceedings initiated at the request or initiative of the data subject, consent shall be deemed to have been given in respect of the personal data necessary for the conduct of the proceedings, where the processing is based on the data subject's consent.

(12) [36]Consent-based processing requires the data subject's written consent (which includes their personally identifiable information and their declaration that, on the basis of the processing notice published by the controller and of which he or she has become aware (name and location of the notice), he or she freely gives their consent to the processing of their personal data by the controller for the purposes and on the legal basis specified therein.

(13) [37]Only personal or specific data which are strictly necessary for the purpose of the case and the purpose of which can be justified may be processed. The data may only be used for the purpose of the case in question and may not be linked to other procedures and data, unless otherwise provided by law.

(14) [38]To ensure data quality, personal data may only be recorded from a valid official identity

[30]REGULATION Article 32
[31]REGULATION Article 5 (1) f)
[32]REGULATION Article 5 (1) f)
[33]REGULATION Article 32
[34]REGULATION Article 32
[35]REGULATION Article 6 (1)
[36]REGULATION Article 7
[37]REGULATION Article 5 (1) b)
[38]REGULATION Article 5 (1) d)

card that identifies the data subject, and specific data may only be recorded with the written consent of the data subject.

(15) [39]During the collection and further processing of data, care must be taken to ensure the accuracy, completeness and timeliness of personal data so that the rights of data subjects are not adversely affected.

(16) [40]Personal and specific data not included in the file, which are recorded in a paper record, must be rendered unidentifiable in order to prevent their further use. Working copies generated during the computerised process, or copies that have been corrupted or become redundant for any other reason, must be destroyed.

1.8. General purposes of processing, processing documents and records

(1) [41]The University processes data for administrative and record-keeping purposes on the basis of a different purpose.

(2) The records and documents required by this Policy shall be kept and prepared by the Local Data Protection Officer. The head of the department appointing the local data protection officer is responsible for the completeness of the records and the accuracy and timeliness of the data contained therein.

1.9. Records of processing activities

(1) [42] The processing of personal data at the University takes place after the registration of the data processingin accordance with Article 30 of the Regulation.

(2) TheUniversity, as data controller, keeps and maintains the data management register in a decentralised manner through the local data protection officers.

(3) The head of the department managing the data file for record keeping purposes shall notify the SAB of the creation of a new data file before the start of the activity. If the ABK or the DPO, in the course of their duties, finds that the processing of personal data requires the keeping of a register, he or she shall inform the head of the department and provide methodological assistance for the performance of the tasks related to the register.

(4) The register of data management shall contain a record of the data management of all parts of the department according to its internal organisation. The department conducts a self-audit built into the process, and the ABK conducts an annual audit to check the adequacy and timeliness of the content of published records. The department shall complete and amend the data management register as necessary. In the case of a ceased processing, the department shall archive the processing records, and in the case of a new processing, it shall establish a new processing record.

(5) The register is published on the websites of the departments that are obliged to designate a local DPO in xls format.

(6) A sample of the data management register is available from the forms library.

[39]REGULATION Article 5 (1) d)
[40]REGULATION Article 5 (1) f)
[41]REGULATION Article 6
[42]REGULATION Article 30

1.10. Transmission of data and record of data transmitted

(1) [43]Personal data shall be disclosed to persons other than the data subject who have explicitly indicated the purposes and legal basis of the processing and who are entitled to access the data by law.

(2) The transfer of data must be recorded in order to establish which data have been transferred or provided by the controller, to whom, under what authority, and when (e.g. domestic legal assistance, etc.). If the entry of a new item in the register is justified where the determination of the legal title is not clear, the ABK will examine the legal basis and the lawfulness of the transfer on the basis of an individual request from the local data protection officer and take a position on the feasibility of the transfer.

(3) The register is kept by the local data protection officer for each department.

(4) The head of the department shall be liable to the data subject for the lawfulness of the transfer in respect of the data he or she processes.

(5) If the transfer cannot be lawfully carried out or if the information necessary for the assessment of the request is not provided by the data subject after the request, the transfer shall be refused.

(6) Any refusal to transfer data shall be notified in writing to the applicant, together with the reasons for the refusal.

(7) In the absence of a legal authorisation for the transfer of data, the data subject shall be asked to give their consent, in writing, in the proceedings initiated at their request, to the transfer of their personal data, in so far as the processing of their case requires the intervention of another body.

(8) The data subject has the right to obtain information about the processing of their personal data and to request the rectification, erasure or blocking of their personal data, except for mandatory processing. Requests for information on data processing must be complied with within a maximum of 30 days, subject to the legal conditions, but preferably without delay.

(9) Personal data may only be transferred or supplied and different processing operations may only be combined if the data subject has given their consent or if required or permitted by law and the conditions for processing are met for each individual personal data item.

(10) The local data protection officer shall review the transfer register by 31 December each year, amend it if necessary and draw up a report on the review. The minutes shall be sent electronically to the ABK by 10 January of the year following the year in question.

(11) The JSA shall publish a specimen of the transmission register drawn up in accordance with Article 30 of the Regulation and a specimen of the record required for the review of the register in the forms library.

1.11. Records of processing activities

(1) [44]Where personal data relating to the data subject are collected from the data subject, the controller shall inform the data subject by means of a privacy notice at the time of obtaining

[43] REGULATION Article 5 (2)
[44] REGULATION Articles 13 and 14

the personal data or, if not collected from the data subject, within a reasonable period of time after obtaining the data, but no later than one month.

(2) The University uses two types of privacy notice:

a) a general information note on data management as a summary of the University's data management activities (preparatory: ABK, publication by the Rector, the Chancellor and the President of the Clinical Centre),

b) individual data processing notices, describing the individual processing activities for each purpose (prepared by the local data protection officer and published by the head of the department responsible for the local data protection officer).

(3) [45]The General Data Protection Notice contains:

a) the name and address of the University,

b) the name and contact details of the University representative,

c) the contact details of the University Data Protection Officer,

d) the purposes for which the personal data is processed by the University,

e) the legal basis for the processing of data by the University,

f) the main categories of personal data processed by the University,

g) the main categories of persons concerned by the processing,

h) the general retention and storage period of the data processed by the University,

i) the general organisational and technical measures taken by the University to ensure data security,

j) the data protection incidents and risks that may occur in the course of the University's data processing and the measures taken to address these risks,

k) the recipients of the personal data services regularly provided by the University,

l) the categories of joint controllers and processors used in the University's data processing activities and the nature of their activities.

(4) [46]General data management information by categories of data subjects

a) the processing of employees' data,

b) the processing of students' data,

c) on the processing of health data,

d) data processing for research purposes,

e) the processing of personal data that contains personal rights protected by specific legislation

information leaflets.

(5) [47]In addition to paragraph 3, the specific privacy notice shall contain the following information about the University's

a) the purposes for which the personal data are processed for the purposes for which they are processed,

b) the legal basis for processing the data for the purposes for which they are processed,

c) the categories of personal data processed for the purposes for which they are collected,

[45] REGULATION Article 13
[46] REGULATION Article 13
[47] REGULATION Article 13

d) the categories of persons concerned by the processing for the purposes for which it is intended,
e) the general processing and retention period of the data processed,
f) the general organisational and technical measures taken to ensure data security,
g) the data protection incidents and risks that may occur in the course of processing for the purposes for which the data are processed and the measures taken to address those risks,
h) the recipients of the data transfers for the purposes for which they are processed,
i) the names and activities of the joint controllers and processors used for the purposes of the processing.

(6) [48]The University provides information about its data management activities to the data subject by means of the data management notices published on its website.
a) The General Data Protection Notices are published by the ABK on the main page of the University's website.
b) The specific privacy notices are available on the main page of the website of the department responsible for the designation of the local DPO, on the website of the Directorate-General for Legal and Administrative Affairs (hereinafter: JIF) website, and a link to them must be provided.

(7) [49]A record of the publication of specific privacy notices shall be kept with the following content
a) the file number of the privacy notice,
b) the title of the privacy notice,
c) the date of publication of the privacy notice,
d) the title of the privacy notice,

(8) [50]The local data protection officer shall review the register of individual data protection notices by 31 December each year, amend it if necessary and draw up a report on the results of the review. The minutes shall be sent electronically to the ABK by 10 January of the year following the year in question.

(9) The model of the ABK register and the model of the record required for the review of the register are published in the forms library.

1.12. Disposition register

(1) [51]The local data protection officer shall exercise the rights of the data subject provided for in Articles 15 to 22 of the Regulation
a) information,
b) access,
c) correction,
d) limitations,
e) delete/forget,

[48] REGULATION Article 5 (2)
[49] REGULATION Article 5 (2)
[50]REGULATION Article 5 (1) d)
[51] REGULATION Article 5 (2)

f) data portability,
g) protest,
h) contribution

keep a register of allocations by department.

(2) The local data protection officer shall review the Register of Administrations by 31 December each year, amend it if necessary and draw up a report on the results of the review. The minutes and their annexes shall be sent electronically to the ABK by 10 January of the year following the year in question.

(3) The model of the ABK register and the model of the record required for the review of the register are published in the forms library.

1.13. Register of processors, joint controllers, data processing

(1) Processing, joint processing and third-party processing contracts concluded by the University for a third-party controller are also subject to the opinion of the ABK in the context of the legal opinion.

(2) The ABK shall keep a register of contracts within the meaning of paragraph 1, which shall include
   a) the name, address and representative of the data processor, joint controller, data controller, data processor or data controller;
   b) the name and contact details of the data protection officer of the data processor, joint controller or data controller or data controller organisation;
   c) the purpose of the processing;
   d) the legal basis for the processing of data for the purposes of data management and processing;
   e) the categories of personal data processed for the purposes of processing;
   f) the categories of persons concerned by the processing for the purposes of the processing;
   g) the scope of the agreement on data processing;
   h) the University department concerned.

(3) The processing shall be subject to an agreement pursuant to Article 28 of the Regulation and the joint controllers to an agreement pursuant to Article 30 of the Regulation as a sub-contract to the basic contract. A sample of this will be published by the ABK in the forms library.

1.14. Data protection incidents and their recording

(1) [52]Employees are required to report suspected data breaches (hereinafter referred to as "incidents") to the local data protection officer (or, in the absence of such officer, to the head of the department) within 24 hours of becoming aware of them.

(2) The Local Data Protection Officer shall report the incident in writing to the DPO and the Information Security Officer no later than 36 hours after becoming aware of the incident.

[52] REGULATION Article 33

(3) If the deadline is not met, the head of the department concerned will prepare a supporting report to the Rector and the Chancellor, who will decide on the further action to be taken after consulting the DPO.

(4) [53]The University, through the Data Protection Officer, shall keep a record of the personal data concerned, the number and type of data subjects affected by the incident, the date of the incident, the circumstances, the effects and the measures taken to remedy the incident, and other data specified in the legislation requiring the processing, for the purpose of monitoring the measures taken in relation to the incident and informing the data subject.

(5) [54]Within 48 hours of the notification, the DPO will decide whether the University has a reporting obligation in relation to the incident. If the University is required to report to the data protection authority, the report will be prepared for decision by the Rector and the Chancellor so that the report can be made within 72 hours.

(6) [55]The DPO will investigate the incident when assessing the risk:

a) the nature of the data breach,
b) the scope and approximate number of persons concerned,
c) the categories and approximate number of data affected by the incident,
d) the name and contact details of the local data protection officer or other contact person who can provide further information,
e) the likely consequences of the incident,
f) the measures taken or planned to remedy the incident, including, where appropriate, measures to mitigate any adverse consequences of the incident.

(7) The forms necessary for the notification of an incident to the DPO, for the assessment of the incident, for the decision on the handling of the incident, for the notification of the incident to the supervisory authority, for informing the data subjects about the incident are published by the ABK in the forms repository.

(8) [56]The DPO shall, at the discretion of the Rector and the Chancellor, notify the supervisory authority of the occurrence of an incident, if the incident is likely to pose a risk to the rights of the data subject, within 72 hours of becoming aware of it.

(9) [57]If the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, the University shall inform the data subject, in accordance with the Rector's decision, without undue delay and within a maximum of 30 days.

(10) The local data protection officer shall review the incident records kept by them by 31 December each year, amend them if necessary, and draw up a report on the results of the review, which shall be sent electronically to the JPC by 10 January of the following year.

(11) The ABK shall publish a model of the incident management register and the record required for the review of the register in the forms repository.

[53] REGULATION Article 5 (2)
[54] REGULATION Article 33 (1)
[55] REGULATION Article 33 (3) Article 39 (19) d)
[56] REGULATION Article 33 (1)
[57] REGULATION Article 34

1.15. Local data protection officers and their records

(1) In 1.3. the head of the department required to be designated pursuant to Section (2) shall inform the ABK within 8 days of the designation of the local data protection officer and of the withdrawal of the designation.
(2) The ABK keeps a register of local data protection officers.
(3) The register contains the following:
   a) name of the organisational unit
   b) the name, position and contact details of the local data protection officer,
   c) the date of designation/revocation of designation of the local data protection officer.

2. ENSURE THE RIGHTS OF DATA SUBJECTS WITH REGARD TO DATA PROCESSING

2.1. Ensuring the rights of the data subject

(1) The University will facilitate the exercise of the rights of the data subject. In order to exercise their rights, the data subject is required to prove their identity and their eligibility at the time of the request. If the application is not made by the person entitled to make the application or if the applicant cannot be identified, the application shall be rejected. The application must be submitted using the form in the Annex to the Rules, which is freely accessible to all on the JIF website.
(2) The application must be sent electronically to adatvedelem@semmelweis.hu or by post to the following address: Semmelweis University Centre for Data Protection and Patient Rights 1428 Budapest, Pf. 2.
(3) If the application is submitted to another department of the University, it must be forwarded to the ABK within three working days.
(4) If the application is incomplete, the ABK will invite the applicant to submit a request within 8 days. The deadline for completing the application does not count towards the 8-day transmission deadline or the 30-day deadline for completing the application.
(5) Within 8 working days, the JHA will send the request, together with its opinion on the eligibility of the applicant and the feasibility of the request, to the department involved in its execution.
(6) The head of the department shall inform the person concerned of the action taken on the request without undue delay and within a maximum of 30 days of receipt of the request.
(7) Taking into account the complexity of the application and the number of requests, the deadline may be extended by a further two months if necessary. The ABK and the department involved in the execution of the application are also entitled to extend the deadline.
(8) The head of the department shall inform the person concerned of the extension of the deadline, stating the reason for the delay, within one month of receipt of the request, and at the same time inform the ABK. Where the data subject has made the request by electronic means, the information shall be provided by electronic means where possible, unless the data subject requests otherwise.

(9) The head of the department examining the application shall inform the applicant and the ABK in writing of the rejection of the application within one month of its receipt, stating the reasons for the rejection.

(10) The local data protection officer keeps a record of the requests received and their execution or rejection. The register contains the following:
   a) the file number,
   b) the identity data of the applicant,
   c) the subject of the request and the type of right concerned,
   d) the receipt date of the request,
   e) the date and time of the request fulfillment,
   f) the reason and date of refusal,
   g) the period of time needed to process the application.

2.2. Information to data subjects

(1) [58]In order to ensure that data subjects are properly informed about all data processing, the University will issue a privacy notice.

(2) In addition to the information contained in the register on the processing of personal data, the information notice shall contain information on the fact that the data subject
   a) have the right to obtain confirmation and information about the data processed about them,
   b) how they can exercise their rights in relation to the processing,
   c) may request the controller to access, modify, rectify, erase or restrict the processing of personal data concerning him or her and may object to the processing of such personal data,
   d) request the portability of their data from the controller,
   e) may withdraw their consent to processing at any time, without prejudice to the lawfulness of the processing carried out on the basis of the consent prior to its withdrawal,
   f) may lodge a complaint with the supervisory authority to protect their rights,
   g) whether the provision of personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract,
   h) is obliged to provide the personal data and the possible consequences of not providing the data.

(3) In the case of data processing in accordance with a legal provision, the performance of a task carried out in the public interest or in the exercise of official authority, the fulfilment of a legal obligation concerning the University, a contractual obligation, its own legitimate interests or the legitimate interests of third parties, or the interests of the data subject, the University provides the information electronically; the University makes the information available on its central website. The University shall inform data subjects of the location of the accessibility of the information notice for all processing.

[58] REGULATION Article 15

(4) In the case of processing based on the data subject's consent, the information notice must be given to the data subject - by receipt, postal delivery, electronic mail - and the document certifying receipt must be kept with the processing. The information shall be given to the data subject before the data are collected from them, in order to ensure transparent information, communication and appropriate measures for the exercise of the data subject's rights. Where the data do not originate from the data subject, the data subject must be informed within 30 days.
(5) The head of the department responsible for the designation of the local data protection officer is responsible for providing the information.

2.3. Ensuring the right to modify and rectify data

(1) In granting the right of rectification, the data subject shall have the right to obtain from the University, upon their request, the rectification or correction of personal data relating to them without undue delay. Taking into account the purpose of the processing, the data subject has the right to request the completion of incomplete personal data, including by means of a supplementary declaration.
(2) Modification or deletion of health data should only be carried out in such a way that the data originally recorded remains legible.
(3) The head of the department handling the data is responsible for the correction of the data.

2.4. Ensuring the right to erasure

(1) In granting the right of rectification, the data subject shall have the right to obtain from the University, upon their request, the rectification or correction of personal data relating to them without undue delay.
   a) whether the processing of personal data is still necessary for the purposes for which they were collected or otherwise processed,
   b) whether the data subject has withdrawn the consent on which the processing is based and whether there is another legal basis for the processing,
   c) whether the data subject has objected to the processing and there is no overriding legal ground for the processing,
   d) the processing is for direct marketing purposes and whether the data subject has objected to the processing,
   e) whether the personal data was unlawfully processed,
   f) whether the personal data must be erased to comply with a legal obligation under Union or Member State law to which the controller is subject,
   g) whether the personal data was collected in connection with the provision of information society services.
(2) If the conditions for the deletion of the data are met, the University will carry out the deletion without undue delay in accordance with the data subject's request.
(3) If the processing of the data is required and authorised by law, the controller shall inform the data subject of this at the same time as the refusal of the request.
(4) The head of the department that processed the data is responsible for deleting the data.

2.5. Ensuring the right to restriction of processing

(1) In exercising the right to restriction of processing, the data subject shall have the right to obtain from the University, at their request and without undue delay, the restriction of processing in the following cases:
   a) where the data subject contests the accuracy of the personal data, the restriction applies for the period of time necessary to allow the controller to verify the accuracy of the personal data,
   b) where the processing is unlawful and the data subject opposes the erasure of the data and has instead requested the restriction of their use,
   c) the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims,
   d) the data subject has objected to the processing; in this case, the restriction applies for the period until it is established whether the legitimate grounds of the controller override those of the data subject.

(2) The University shall, where the conditions for the restriction of processing are met, act on the data subject's request without undue delay.

(3) The head of the department processing the data is responsible for restricting the processing.

2.6. Ensuring the right to data portability

(1) In exercising the right to data portability, the data subject shall have the right to obtain from the University, upon their request and without undue delay, an examination of whether
   a) processing is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into the contract; or
   b) is based on the consent of the data subject.

(2) Where the conditions for data portability are met, the University shall, without undue delay and in accordance with the data subject's request,
   a) provide the data in a structured, commonly used, machine-readable format,
   b) transfer the data directly to the controller designated by the data subject.

(3) The head of the department processing the data is responsible for the transmission of the data.

2.7. Ensuring the right to object to processing

(1) In ensuring the right to object to processing, the data subject shall have the right to have the University examine, at their request and without undue delay, whether the right to object to processing is enforceable, i.e
   a) whether the processing was necessary for the performance of a task carried out in the public interest,
   b) whether the processing was necessary for the purposes of the legitimate interests pursued by the controller or a third party.

(2) If the conditions for exercising the right to object to processing are met and there is no other legal basis for processing the data, the University shall, in accordance with the data subject's instructions, cease processing the data without delay.
(3) The head of the department processing the data is responsible for the termination of data processing.

2.8. Ensuring the right of access to data

(1) Under the right of access, the data subject has the right to obtain from the controller information as to whether or not their personal data are being processed and, if such processing is taking place, the right to access the personal data and the following information:
   a) the categories of personal data concerned;
   b) the purposes of the processing;
   c) the recipients or categories of recipients to whom or which the personal data have been or will be disclosed, including in particular recipients in third countries and international organisations;
   d) the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period;
   e) may request the controller to rectify, erase or restrict the processing of personal data concerning them and may object to the processing of such personal data;
   f) have the right to lodge a complaint with a supervisory authority;
   g) if the data were not collected from the data subject, any available information on their source;
   h) the fact of automated decision-making, including profiling, as referred to in Article 22 (1) and (4) of the Regulation and, at least in those cases, the logic used and clear information on the significance of such processing and its likely consequences for the data subject.
(2) Where personal data are transferred to a third country or an international organisation, the data subject is entitled to be informed of the appropriate safeguards for the transfer in accordance with Article 46 of the Regulation.
(3) The head of the department processing the data is responsible for the transmission of the data.

2.9. Examination of the legal basis for processing

(1) [59]Each year, the University examines the documentation of all personal data processing recorded in the data management register to ensure that the data contained therein have been processed in accordance with the law and the University's policies, that the appropriate legal basis for the processing continues to exist, and that the data are processed on the basis of the appropriate legal basis. The head of the department shall act on the basis of the ABK's methodological guidelines as regards the legal basis for data processing.

[59] REGULATION Article 5 (1) a) and Article 6

(2) When examining the processing of any data, the legal basis for the processing and whether the documentation supporting the legal basis for the processing is available must be established. If necessary, the ABK will assist you in establishing the legal basis.

(3) [60]The legal basis for the University's processing and the necessary documentation:

a) data processing based on the data subject's consent: processing based on the data subject's or their legal representative's freely given and explicit indication of his or her wishes, based on adequate information (purpose, legal basis, duration, name of the controller, address of the processor and the activity for which the data are processed) and by which the data subject gives his or her unambiguous consent to the processing of personal data concerning him or her, whether in full or in part;

b) processing necessary for the performance of a contract concluded or to be concluded with the data subject: the contract concluded with the data subject - a declaration on the conclusion of the contract (indicating in the contract the processing necessary or by means of a separate sheet of paper which processing is necessary for the performance of which provision of the contract);

c) processing necessary for compliance with a legal obligation to which the controller is subject: the precise legal provision imposing or requiring the processing;

d) processing necessary to protect the vital interests of the data subject or of another natural person: whether the balancing of interests test has been carried out

da) the purpose of the processing,

db) whether the processing of personal data is absolutely necessary for the purposes of the data subject or another natural person,

dc) whether alternative means are available to achieve the intended purpose without processing personal data,

dd) the most precise possible definition of legitimate interest,

de) what personal data, and for how long the legitimate interest requires the processing,

df) what the other party's interests are that may legitimately ensure that the processing is based on the other party's interests;

e) processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller: the precise name and text of the legal provision defining the public interest of the controller or the official authority vested in the controller and the necessity of the processing determined by that authority;

f) [61]necessary to pursue the legitimate interests of the controller or a third party: whether the balancing of interests test has been carried out,

fa) is necessary for the controller or a third party to achieve its purposes whether the processing of personal data is necessary,

fb) whether alternative means are available to achieve the intended purpose without processing personal data,

fc) the most precise possible definition of legitimate interest,

[60]REGULATION Article 6

[61] REGULATION Article 6 (1) f), Preamble (69).

fd) the purpose of the processing,
fe) how long the legitimate interest requires the processing of personal data,
ff) what the other party's interests are that may legitimately ensure that the processing is based on the other party's interests;

(4) [62]When documenting the processing based on consent, it should be verified that
a) the documentation supporting the legal basis is available and has been obtained lawfully,
b) whether consent was the appropriate legal basis for processing the data,
c) the consent has been given in the correct form,
d) whether the data subject has received appropriate information before giving consent.

(5) The University provides the data subject with the right to withdraw, modify or restrict his or her previous declaration by making available on its website the form "REQUEST FOR THE APPLICATION OF THE RIGHTS OF CONTROL", which can be downloaded without any limitation.

(6) The local data protection officer is responsible for examining the legal basis for the processing.

2.10. Special data management

(1) The University shall process sensitive data only if one of the conditions set out in Article 9 (2) of the Regulation is met.

(2) [63]When processing special categories of personal data, the Local Data Protection Officer will check, in each processing operation, that the processing based on consent has been carried out in accordance with the data processing rules. The ABK's position on the compliance of data processing with the law shall prevail.

2.11. Ensuring data leakage prevention

(1) [64] The University has appropriate procedures to prevent, detect, report and investigate data leaks.

(2) The University will take the following measures to prevent the leakage of personal data in accordance with the Information Security Policy:
a) assess the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data,
b) investigate the ability to restore access to and availability of personal data in the event of a physical or technical incident in a timely manner,
c) establish a procedure for the regular testing, evaluation and assessment of the effectiveness of the technical and organisational measures taken to ensure the security of data processing in the context of information security,
d) carry out a risk analysis to determine the appropriate level of security in order to identify the risks of accidental or unlawful destruction, loss, alteration, unauthorised

[62] REGULATION Article 7
[63] REGULATION Article 9
[64] REGULATION Article 32

disclosure of or access to personal data transmitted, stored or otherwise processed and the damage they may cause.

3. THE UNIVERSITY'S DATA PROTECTION SYSTEM

3.1. The Data Protection Officer

(1) [65]The Chancellor, in agreement with the Rector, shall appoint an independent Data Protection Officer from the JIF, with a law degree and at least 3 years of experience in data protection, to perform the duties of the University as Data Controller and Data Processor, either by competitive application or by assignment until the application is evaluated.

(2) [66] The University will ensure that the DPO has appropriate and timely access to all matters involving the processing and handling of personal data. In order to carry out their tasks, they have the right to access the data managed by the departments and to request data from the departments.

(3) The University shall provide the DPO with the resources necessary to perform these tasks, to have access to personal data and data processing operations, and to maintain the DPO's level of expertise.

(4) [67]The DPO shall not accept instructions from anyone in connection with the performance of his or her duties. The DPO is directly responsible to the University's top management.

(5) [68,69]

(6) [70]The DPO is bound by confidentiality obligations in the context of his or her activities, regardless of the duration of the legal relationship and without any time limit.

(7) The Data Protection Officer's tasks include in particular:

a) to provide information and technical advice to the controller or processor,

b) to monitor the implementation of the data protection legal governance tools and compliance with the rules on the basis of an annual work plan, reporting annually to the Rector and the Chancellor,

c) professionally supervise staff training on data protection,

d) on request, provide technical advice on the data protection impact assessment and monitor the conduct of the impact assessment,

e) cooperate with the supervisory authority,

f) act as a contact point for the supervisory authority on matters relating to data processing, including prior consultation, and consult it on any other matter as appropriate,

g) contribute to the University's integrated risk assessment to identify data protection risks,

h) as part of their advisory role, they propose the topics for training on data protection.

---

[65] REGULATION Article 37 (5), (6).
[66] REGULATION Article 39
[67] REGULATION Article 38 (3)
[68] REGULATION Article 38 (6)
[69] Repealed by Senate Decision 54/2023 (29 June) Annex 2 Article 1 Effective from: 11 July 2023
[70] REGULATION Article 38 (5)

i) [71]assists the data subject in exercising his or her rights and initiates the measures necessary for the controller to investigate and remedy the complaint.

(8) The Data Protection Officer is entitled to the following:
   a) inspect all processing covered by this policy and enter any premises where processing is taking place,
   b) request information and clarification on any processing covered by this Policy,
   c) participate with the right of deliberation and approval in all forums of the University and its departments where matters within their competence are on the agenda.

3.2. The Center for Data Protection and Patient Rights (ABK).

(1) The ABK operates as a department of the JIF under the direction of the Director General of the JIF and under the professional supervision of the Data Protection Officer.
(2) The ABK is managed by the Director of Privacy and Patient Rights.
(3) The role of the ABK in the process of regulation:
   a) regularly reviewing policies on data management and data security and ensuring that they are up to date,
   b) preparing and publishing in the forms library the forms provided for in these Rules,
   c) participating and providing professional advice to departments in the preparation and updating of the data management parts of the rules and regulations, including rules on data management.
(4) The role of the ABK in advising:
   a) to provide guidance and individual consultation to local data protection officers and departmental managers on the practices of data protection and patient rights procedures within the University (complaint handling, data disclosure, record keeping),
   b) to prepare methodological guides,
   c) to assist the University's Information Security Officer by providing advice on data protection aspects of the authorisation and approval procedures within the scope of their activities.
(5) The responsibilities of the ABK in relation to complaints and notifications from data subjects are set out in the relevant internal rules.
(6) The role of the ABK is to monitor the following:
   a) if unlawful data processing is reported or detected, participate in its investigation and assist in its elimination,
   b) monitor the activities of departments and local data protection officers in relation to data protection tasks.
(7) The role of the ABK is to organise training:
   a) preparing a training curriculum based on a proposal from the DPO,
   b) preparing data protection training material for new staff members based on the data protection training theme,
   c) organising training for local data protection officers,

[71] REGULATION Article 38 (4) plus “Infotv.” Article 25/M

d) in the event of legislative changes, organising information depending on the nature and scope of the change.

(8) The ABK contributes to the review of contracts concerning data protection and the processing of personal data under the University's Contract Regulations.

(9) In order to carry out their tasks, the staff of are entitled to access the data managed by the departments and to request data from the departments. The staff of the ABK are bound by confidentiality obligations in connection with these activities, regardless of the duration of their employment relationship.

3.3. Designation and tasks of the local data protection officer

(1) The head of the department that is required to designate a local data protection officer is responsible for the data management activities of the department(s) under his or her control.

(2) Head of the department responsible for designating the local data protection officer
   a) designates a local data protection officer,
   b) monitors their activities at regular intervals through reporting,
   c) decides on the further storage or destruction of the recorded data after the mandatory retention period.

(3) The Local Data Protection Officer must be a person with professional competence and, in particular, expert knowledge of data protection law and practice, and be able to perform the tasks required by law.

(4) The local data protection officer
   a) ensures the preparation, maintenance, publication and review of the department's records and information on data management, and informs the ABK of the results of the review in accordance with the provisions of these Rules,
   b) organises data protection training for persons involved in data management and processing in the department,
   c) assists in responding to complaints about the processing of personal data by the department, at the request of the ABK,
   d) provides information on complaints, data requests and action taken when requested by the ABK,
   e) inform the DPO of the suspected data breach that has occurred,
   f) provides data to the JIF in response to requests for public interest data received by the department or found within the department.

(5) In the absence of the designation of a Local Data Protection Officer, the Head of the department authorised to designate a Local Data Protection Officer shall perform the duties of the Local Data Protection Officer as set out in these Rules.

3.4. The data protection monitoring system

(1) [72]The Rector, the Chancellor, the President of the Clinical Centre, through the Data Protection Officer and the ABK, review the implementation of the legislation on data

[72] REGULATION Article 39; Article 5 (2)

management and protection. The Data Protection Officer prepares an annual information report on the current state of data protection for the Rector, the Chancellor and the President of the Clinical Centre by 1 February each year.

(2) Departments review their own data management processes and their compliance through in-process self-audits.

(3) The local data protection officers shall review the records they keep and the published privacy notices by 31 December each year and shall inform the ABK of the results of the review by 10 January of the year following the year in question, as required by these rules.

(4) The DPO shall, on the basis of an annual audit plan, check that the University's departments
   a) comply with their obligations regarding the protection of personal data, in particular
      aa) the obligation to inform data subjects,
      ab) their obligations to ensure the right of access of data subjects,
      ac) their obligations to ensure the rights of data subjects.
   b) comply with their obligations in relation to data breaches,

(5) The Data Protection Officer will keep a record of the inspection and take the following actions:
   a) in the event of a deficiency being detected, call on the head of the department concerned to take action within 15 days, with a deadline of 15 days,
   b) will carry out a follow-up inspection within 30 days of the deadline for action to verify compliance with the action.
   c) Within 15 days of the follow-up check, it verifies the implementation of the measure and, if the measure is not taken or not properly implemented, informs the Chancellor by requesting action.

(6) The ABK examines the annual review reports prepared by the local DPOs and, in case of deficiencies, provides support to ensure compliance through the person designated by the Director General of Legal and Administrative Affairs.

(7) The Revision Directorate acts in accordance with the rules that apply to it when conducting investigations concerning data protection.

4. COMPLIANCE SUPPORT FOR THE UNIVERSITY'S DATA PROCESSING DEPARTMENTS

(1) The JIF Director General has appointed a dedicated staff member to promote data protection compliance, who, in cooperation with the local Data Protection Officer of the department, provides methodological assistance to the departments according to a schedule set by the JIF Director General in prior agreement with the Director of the ABK
   a) the preparation and maintenance of data protection documentation (data protection adequacy audit),
   b) to assess the operational adequacy of departments (data protection operational audit) in accordance with the professional methodological standards set by the DPA,
   c) to ensure the data protection awareness required by this Policy, provide data protection training and assessment to staff members designated by the Head of the department,

on the basis of a proposal from the DPO, according to the training agenda set by the DPO,

d) report regularly to the JIF Director General on updates on compliance support activities.

e) The designated employee shall inform the local data protection officer concerned of his or her availability and the training schedule.

(2) JIF publishes a methodological guide on its website

a) the processing of employees' data,
b) the processing of students' data,
c) the management of health data,
d) tasks relating to the processing of data concerning personal data protected by specific legislation, and
e) on means to support compliance with adequateness and operational audits and training to ensure data protection awareness,
f) to promote data protection compliance for the reserved institutions

(3) The application of the guidelines is mandatory for persons and organisations covered by these Rules and expected for the institutions it covers.

5. Annexes

Annex 1: Types of records, information notes and minutes kept by the local data protection officer

Annex 2: Audit trail

1. Annex ...: Types of records, information notes and minutes kept by the local data protection officer

A) Data processing register - the register referred to in Article 30 of the Regulation to be kept (by type of processing activities):

    1. professional activities
    2. scientific research activities
    3. labour- and human resources activities
    4. administrative activities (economics, secretariat, communication)

B) Data management notices related to the processing register

C) for further records:
    1. register of information on data management
    2. data transmission register
    3. register of contributions by the parties concerned
    4. disposition register
    5. educational register
    6. data protection incident record

D) Minutes
    1. a record of the required maintenance of records
    2. self-inspection report

Annex 2: Audit trail

2/A. Data Protection and Patients' Rights Centre

	process steps	preparation steps	responsibility levels					document resulting from the process
			task host	verification	mode of verification	approval	mode of approval	
1	patient data release	examination of admissability of an application	Designated staff member of the ABK	Head of ABK	document control, signature	Head of ABK	signature	response document
2	carry out an impact assessment	assessment of the need for new processing, consultation of the Data Protection Officer	head of the department concerned, local data protection officer	Head of ABK, Data Protection Officer	data analysis	Head of ABK	signature	impact assessment document
3	centralised patient complaints handling	examination of a referral under the relevant procedure, involving a Clinical Centre	Designated staff member of the ABK	Head of ABK	document control, signature	Head of ABK, President of the Clinical Centre	signature	response document
4	complaints handling at organisational level	assistance on request, taking a position on a given matter	Designated staff member of the ABK	Head of ABK	document control, signature	Head of ABK	signature	response document
5	preparing guidelines	proposal for the publishing of guidelines	Designated staff member of the ABK	Head of ABK	document control, signature	Head of ABK	signature	guidelines document
6	liaising with patients' representatives	scheduled and ad hoc meetings	Head of ABK	n.a.	document control, signature	Head of ABK	signature	reminders
7	record keeping	establishment and ongoing implementation of registers	Designated staff member of the ABK	Head of ABK	document control, signature	Head of ABK	signature	a record with a signature certifying that the inspection has been carried out
8	giving opinions on contracts concerning data	examination of contracts	Designated staff member of the ABK	Head of ABK	document control, signature	Head of ABK	signature	a draft contract that complies with data protection requirements

	process steps	preparation steps	responsibility levels					document resulting from the process
			task host	verification	mode of verification	approval	mode of approval	
	protection and the processing of personal data							
9	monitoring the compliance of university data protection activities	examination of annual minutes prepared by local DPOs, ongoing activities during the year, checking the adequacy of documents received	Designated staff member of the ABK	Head of ABK	reporting	Head of ABK	acceptance of the reports	report on the results of the conformity assessment

2/B Data Protection Officer

	process steps	**preparation steps**	**responsibility levels**					**document resulting from the process**
			task host	**verification**	**mode of verification**	**approval**	**mode of approval**	
1	information and advice	learning about the case, developing a position	the Data Protection Officer	n. a.	n. a.	n.a.	signature	reply letter sent to the requestor
2	monitoring the enforcement of data protection-related legal governance instruments	planning and carrying out annual work plan tasks	the Data Protection Officer	n. a.	n. a.	n.a.	signature	annual information to the Rector and Chancellor
3	monitoring of data processing activities	carrying out tasks in line with the annual work plan	the Data Protection Officer	n. a.	mid-year reporting	n. a.	signature	information note for the Rector and Chancellor
4	handling data breaches	incident detection, assessment,	local data protection officer/data controller, head of department involved in the incident	the Data Protection Officer	analysis of data and information	the Rector, the Chancellor	signature	incident management report, briefing to the Rector and Chancellor, reporting to the supervisory authority as necessary
5	liaison and cooperation with the supervisory authority	gathering and analysing relevant information on a case, complying with reporting obligations	the Data Protection Officer	n. a.	n. a.	the Rector, the Chancellor	signature	report