

Semmelweis University Regulations on Data Protection, Disclosure, and Requests for Data of Public Interest

Effective date: April 1, 2026

Book 1: Data Protection Policy

Table of Contents

Preamble 5
1. GENERAL PROVISIONS 5
1.1. The purpose of the Policy is as follows: 5
1.2. Scope of the Policy 5
1.3. Applicable Laws, Definitions, and Forms 6
1.4. Principles, Legal Basis, and Purpose of Data Processing 6
1.5. Data Protection by Design, Conducting a Data Protection Impact Assessment 9
1.6. Enforcing Data Protection Principles and Ensuring Accountability 10
1.7. Data processing and data security requirements during administrative procedures 12
1.8. General Purposes of Data Processing, Data Processing Documents, and Records 15
1.9. Recording of Data Processing Activities 15
1.10. Data Transfer and Record-Keeping of Transferred Data 15
1.11. Privacy Notices and Their Records 16
1.12. Disposal Register 18
1.13. Registration of Data Processors, Joint Data Controllers, and Data Processing Activities 19
1.14. Data Protection Incidents and Their Recording 19
1.15. Local Data Protection Officers and Their Registers 20
2. Ensuring the rights of data subjects regarding data processing 21
2.1. Safeguarding the Rights of the Data Subject 21
2.2. Informing Data Subjects 22
2.3. Ensuring the Right to Modify and Correct Data 23
2.4. Ensuring the Right to Erasure 23
2.5. Ensuring the Right to Restriction of Data Processing 24
2.6. Ensuring the Right to Data Portability 24
2.7. Ensuring the Right to Object to Data Processing 24
2.8. Ensuring the Right of Access to Data 25
2.9. Review of the Legal Basis for Data Processing 25
2.10. Processing of Special Categories of Data 27
2.11. Ensuring the Prevention of Data Leaks 28
3. The University's Data Protection System 28
3.1. The Data Protection Officer 28
3.2. The Data Protection and Patient Rights Center (ABK) 30
3.3. Appointment and Duties of the Local Data Protection Officer 31
3.4. The Data Protection Oversight System 32
4. Supporting Compliance for the University's Data-Processing Units 33

5. Data Protection Provisions Related to Scientific Research 33
6. Final Provisions 36
7. Appendices 36

Preamble

Semmelweis University (hereinafter: the University) is governed by 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 Health and Related Personal Data (hereinafter: Eüak.), and Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: the Regulation), the University hereby establishes the following rules governing data processing at the University.

Semmelweis University's Regulations on Data Protection, Disclosure, and Requests for Data of Public Interest, Book I: Data Protection Regulations (hereinafter: Regulations on Data Protection, Disclosure, and Requests for Data of Public Interest (AKK), Book I: Data Protection Policy (ASZ), Policy) must be interpreted and applied in accordance with the provisions of the Regulation. The Center for Data Protection and Patient Rights (hereinafter: ABK) provides support to facilitate uniform interpretation and application.

1. GENERAL PROVISIONS

1.1. The purpose of the Policy is as follows:

Article 1

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

1.2. Scope of the Policy

Article 2

(1) The scope of this Policy extends to
   a) all data classified as personal data under applicable laws;
   b) the University and all of its organizational units where personal data is processed;
   c) 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, or any organization with independent legal personality that operates with the University's participation or is related to the University's operations (hereinafter "organization"); however, as the operator, owner, or participating member of these organizations, the University assists them and expects them to establish their own data protection systems in accordance with this policy.

1.3. Applicable Laws, Definitions, and Forms

Article 3

(1) The terms used in this policy correspond to those defined in the applicable laws.

(2) For the purposes of this policy:

a) Organizational units required to appoint a local data protection officer: organizational units classified as Level I in the University's Registry of Organizational Units under the Organizational and Operational Regulations; patient care organizational units (clinics and the András Pető Department of Rehabilitation and Health Care); among other organizations classified as Level I, the University Student Council and the Doctoral Student Council.

(3) The use of the forms published in the form repository—which contain the specified data—is mandatory.

1.4. Principles, Legal Basis, and Purpose of Data Processing

Article 4

(1) The University conducts its data processing activities in accordance with the principles set forth in Article 5 (1) of the Regulation: the principles of lawfulness, fairness, and transparency; the principles of purpose limitation, data minimization, and limited storage; the principle of accuracy; and the principles of ensuring integrity and confidentiality.

(2) The University—in accordance with the principle of data protection by design and by default set forth in Article 25 of the Regulation—implements appropriate technical and organizational measures to ensure that the University's data processing complies with the applicable rules.

(3) All organizational units of the University shall ensure that the University is able to demonstrate compliance with the fundamental principles and the rules governing data processing (the principle of accountability).

(4) In the case of activities involving the processing of personal data, the relevant organizational unit shall perform the duties required of the data controller in accordance with the guidelines established by the data protection officer.

(5) The University processes personal data only if

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

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

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

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

[1] REGULATION, Article 6 paragraph (1) lit. b)
[2]REGULATION Article 6 paragraph (1) lit. c)
[3]REGULATION Article 6 paragraph (1) lit. d)

e) [4]the 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 data controller;

f) [5]the processing is necessary for the legitimate interests of the data controller or 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.

(6) Special categories of personal data may be processed if

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

b) [7]the processing is necessary for the controller or the data subject to fulfill obligations arising from legal provisions governing employment, social security, and social protection, and to exercise specific rights under such provisions, provided that Union or Member State law—which includes appropriate safeguards to protect the data subject's fundamental rights and interests— and a collective agreement under Member State law permits this;

c) [8]the processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent;

d) [9]the processing is carried out in the course of the legitimate activities of a foundation, association, or any other nonprofit organization pursuing political, philosophical, religious, or advocacy purposes, including trade unions, subject to appropriate safeguards, provided that the data processing relates exclusively to current or former members of such an organization, or to persons who are in regular contact with the organization in connection with its purposes, and that the personal data are not made available to persons outside the organization without the consent of the data subjects;

e) [10]the processing is necessary for preventive healthcare or occupational health purposes, for the assessment of an employee's fitness for work, for the establishment of a medical diagnosis, for the provision of health or social care or treatment, or for the management of health or social systems and services, pursuant to Union or Member State law or under a contract with a healthcare 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 the provision of health care, ensuring a high level of quality and safety of medicines and medical devices, and is carried out pursuant to Union or Member State law that provides for

[4]REGULATION Article 6 paragraph (1) lit. e)
[5]REGULATION Article 6 paragraph (1) lit. f)
[6]REGULATION Article 9 paragraph (2) lit. a)
[7]REGULATION Article 9 paragraph (2) lit. b)
[8]REGULATION Article 9 paragraph (2) lit. c)
[9]REGULATION Article 9 paragraph (2) lit. d)
[10]REGULATION Article 9 paragraph (2) lit. h)
[11]REGULATION Article 9 paragraph (2) lit. i)

appropriate and specific measures to safeguard the rights and freedoms of the data subject, in particular with regard to professional confidentiality;

g) [12]Data processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, based on Union or Member State law that is proportionate to the objective to be achieved, respects the essence of the right to the protection of personal data, and provides for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.

(7) [13]The data subject must be informed prior to the collection of the data as to the legal basis for the data processing in accordance with Articles 13 and 14 of the Regulation. This is done through the publication of a privacy notice.

(8) [14]Based on consent, when the data subject gives their voluntary, explicit, informed, and unambiguous consent to the processing of data concerning them.

a) Consent covers all data processing activities carried out for the same purpose or purposes.

b) In the case of data processing for multiple purposes, consent must be given separately for each data processing purpose.

c) Consent may only be used for data processing where compliance with the requirements for prior information and the voluntary nature of the consent can be demonstrated. Voluntary consent cannot be demonstrated if consent to data processing that serves exclusively the University's interests was given by data subjects en masse, within a specific group of individuals, and without exception, in a relationship of subordination.

d) Consent may be given in any form that allows the data subject to be identified and the fact of consent to be recorded;

e) Consent cannot be given verbally or over the phone

f) Consent may be given, in particular:

fa) in writing (with the data subject's signature);

fb) electronically, following the individual identification of the data subject (e.g., through the student information system), provided that the fact of consent is recorded (logged);

fc) electronically in a message sent from the data subject's email address registered with the University, provided that the message is recorded and preserved without alteration.

(9) The local data protection officer shall maintain a record of the consents given by data subjects containing the following information:

a) the name and reference number of the data processing register,

b) the reference number of the data processing consent,

c) the natural person's identifying information,

d) the date the data processing consent was granted,

e) the reference number of the data processing notice,

f) the date of withdrawal of the data processing consent.

[12]REGULATION Article 9 paragraph (2) lit. j)
[13]REGULATION Article 12 paragraph (1)
[14]REGULATION Article 7

(10)[15] Employees engaged in data processing at the University's organizational units are required to keep personal data obtained in the course of their work confidential indefinitely, in accordance with Article 8 paragraph (4) of Act I of 2012 on the Labor Code, the Health Care Act (Eütv.), the Health Care Act on Personal Data (Eüak), and other regulations imposing a duty of confidentiality. Confidentiality does not extend to the disclosure of data of public interest, the statutory obligations to provide data and information regarding data of public interest, complaints, or reports in the public interest.

(11)[16] When a new employee joins the University, they receive basic data protection training as part of their onboarding package. Further training and continuing education are organized by the ABK. The local data protection officer maintains a record of employee training containing the following information:

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

1.5. Data Protection by Design, Conducting a Data Protection Impact Assessment

Article 5

(1) [17]At the request of the local data protection officer, prior to commencing new data processing activities (particularly when new data processing technologies are used), if such activities are likely to pose a high risk to the rights and freedoms of natural persons, the ABK shall conduct an impact assessment to determine how the planned data processing operation affects the protection of personal data.

(2) When conducting a data protection impact assessment, the ABK is required to seek the professional advice of the data protection officer.

(3) An impact assessment must be conducted in the following cases:

a) when certain personal characteristics of natural persons are subject to systematic and extensive evaluation based on automated data processing—including profiling—and such evaluation forms the basis for decisions that produce legal effects on the natural person or similarly significantly affect the natural person,

b) in the case of large-scale, systematic monitoring of public areas, such as when using electronic surveillance systems (cameras) that meet these criteria;

c) in the processing of large volumes of health and other special categories of data; in cases of data processing activities listed in the supervisory authority's list of activities for which a data protection impact assessment is mandatory.

d) If the data protection impact assessment determines that the planned data processing—in the absence of measures taken to mitigate risks—would indeed entail a high risk, the data protection officer shall consult with the supervisory authority prior to processing the personal data.

[15]Article 8 (4) of Act I of 2012, 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 paragraph (1) lit. b)
[17]REGULATION, Articles 25 and 35

(4) The University continuously ensures that its internal policies, work instructions, and contracts comply with data protection regulations. Prior to the issuance of policies, instructions (internal regulatory documents), work instructions, and model contracts, the opinion of the ABK must be sought on matters related to the processing of personal data. When authorizing policies and instructions, the authorization under the Regulation must be specified, if relevant.

1.6. Enforcing Data Protection Principles and Ensuring Accountability

Article 6

(1) [18]The University may process personal data if:

a) Data processing is required by law (mandatory data processing). Such data processing includes, in particular, data processing related to higher education activities, employment, public education activities, or the provision of health care services.

b) Data processing is necessary to fulfill a legal obligation. Such data processing includes, in particular, processing that is strictly necessary to fulfill an obligation prescribed by law (e.g., reporting data).

c) The data subject has given consent to the data processing in accordance with the provisions of Article 4 paragraph (8) lit. a)- (1)c) . Such data processing includes, in particular, data processing related to the sending of newsletters based on voluntary subscription, participation in various events and sweepstakes, the completion of questionnaires, or participation in scientific research.

d) The data processing is necessary for the performance of a contract to which the data subject is a party, or for taking steps at the data subject's request prior to entering into a contract. Such data processing may include, in particular, data processing carried out in the course of a service provided by a university that is available on a voluntary basis.

e) The processing is necessary to protect 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 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) [19]In order to ensure compliance with the principles of data processing, the University takes the following measures when processing personal data:

a) [20]Legality, Fairness, and Transparency: The processing of personal data must be carried out lawfully, fairly, and in a manner that is transparent to the data subject. When processing personal data, natural persons must be provided with transparency regarding the legal basis, manner, and method of collecting and using their personal data, the scope of the data processed, as well as the possibility and method of accessing such data. To ensure that the processing of personal data is transparent to the data subject, the local data protection officer maintains a data processing register at for each

[18] REGULATION Article 5 paragraph (2), Article 5 paragraph (1), and Article 6
[19] REGULATION Article 5 paragraph (2), Article 5 paragraph (1), and Article 6
[20]REGULATION Article 5 paragraph (1) lit. a)

data processing purpose, prepares a data processing notice for every data processing activity recorded therein, and makes these notices publicly available without restriction on the organizational unit's sub-website.

b) [21]Purpose Limitation: Personal data may be collected only for specified, explicit, and legitimate purposes. Personal data may not be processed in a manner incompatible with these purposes.

c) [22]Data minimization: Personal data must be adequate and relevant to the purposes of the processing and must be limited to what is necessary.

d) [23]Accuracy: Personal data must be accurate and up-to-date; that is, all reasonable measures must be taken to ensure that personal data that is inaccurate in light of the purposes of the processing is erased or rectified without delay.

e) [24]Limited Storage: Personal data must be stored in a form that allows for the identification of data subjects only for as long as is necessary to achieve the purposes of the processing; personal data may be stored for a longer period only if the processing of such data remains demonstrably necessary thereafter. To ensure that the storage of personal data is limited to the necessary period, the University establishes a data erasure deadline in its records management policy for all data processing activities and records this deadline in its data processing register.

f) Integrity and Confidentiality: The processing of personal data must be carried out in such a way that appropriate technical and organizational measures are implemented to ensure the adequate security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.

g) [25]Accountability: The ABK provides practical assistance in designing the processes involved in data processing in accordance with the provisions of this policy to ensure compliance. The Data Protection Officer reviews compliance with data protection requirements according to an annual work plan, while the ABK conducts ongoing reviews throughout the year in connection with specific matters. The ABK regularly verifies the current status of compliance through the annual self-assessment reports prepared by local data protection officers.

[21]REGULATION Article 5 paragraph (1) lit. b)
[22]REGULATION Article 5 paragraph (1) lit. c)
[23]REGULATION Article 5 paragraph (1) lit. d)
[24]REGULATION Article 5 paragraph (1) lit. e)
[25]REGULATION Article 5 paragraph (2)

1.7. Data processing and data security requirements during administrative procedures

Article 7

(1) [26]In accordance with the provisions of the Information Act, the Decree, and these regulations, University staff members are required to keep documents containing personal data in a locked cabinet outside of working hours—and, whenever possible, during working hours as well. Official documents may be kept on desks or elsewhere in the office only for the purpose of performing work and only during working hours.

(2) [27]Documents containing personal data held by the administrative officer or in the records office may be accessed by persons other than the administrative officer and the administrative officer's supervisor only if permitted by law or if the person submits a request to the administrative officer demonstrating that such access is necessary for the performance of duties related to their work.

(3) [28]In the absence of statutory authorization, data may be transferred to a third party only with the data subject's consent. If the data subject does not consent to the transfer of their data to another entity, they must be informed that, in this case, their request cannot be fulfilled, or cannot be fulfilled in its entirety.

(4) When transferring data within the university, the party requesting the data must always justify the purpose and legal basis of the data request. The data may only be transferred after this has been verified.

(5) [29]When the data subject or their representative exercises their right of access, the process must be conducted in such a way that the rights of others are not infringed (personal or protected data relating to other individuals must be redacted or otherwise rendered unrecognizable). The same procedure must be followed when preparing copies or extracts.

(6) [30]The administrative officer in whose possession the documents listed in paragraph (1) are found at the end of the workday is responsible for securing them. In addition to other considerations, for data protection reasons, rooms where shared printers or copiers are in operation must be used in accordance with data security requirements.

(7) [31]In addition to other considerations, for data protection reasons, rooms where computers or workstations are in operation must be used in a manner that complies with data protection, fire safety, and IT security requirements. The administrative staff member is required to handle and store the computer and its associated data storage media in such a way that data requiring protection cannot be accessed by unauthorized persons. Furthermore, at the end of the workday, the staff member is required to shut down the workstation—with the exception of workstations that must remain continuously powered on and online—and lock the door.

(8) [32]Documents containing personal data may only be removed from University premises—except when necessary for the performance of job duties—with the permission of the

[26]REGULATION Article 5 paragraph (1) lit. f)
[27]REGULATION Article 5 paragraph (1) lit. f)
[28]REGULATION Article 6 paragraph (1)
[29]REGULATION Article 5 paragraph (1) lit. f)
[30]REGULATION Article 32
[31]REGULATION Article 5 paragraph (1) lit. f)
[32]REGULATION Article 5 paragraph (1) lit. f)

immediate supervisor. In such cases, the administrative staff member is also required to ensure that the document is not lost, damaged, or destroyed, and that its contents do not come to the knowledge of unauthorized persons.

(9) [33]Data that is no longer necessary to achieve the purpose of data processing, or for which the purpose of data processing has ceased or been modified, must be destroyed immediately—in accordance with the provisions of the Records Management Policy—or upon the expiration of the prescribed retention period. The destruction of other records containing personal data must also be carried out with the necessary security measures in place.

(10) [34]With regard to individual records and data processing activities, the head of the organizational unit must define access rights on a per-person and per-job-function basis, in accordance with the provisions of the Information Security Policy.

(11) [35]In proceedings initiated at the request or on the initiative of the data subject, with respect to the personal data necessary for conducting the proceedings—provided that the basis for data processing is the data subject's consent—such consent shall be deemed to have been given.

(12) [36]For data processing based on consent, the data subject's written consent must be obtained (which must include the data subject's personally identifiable information, as well as a statement that, based on the privacy notice published by the data controller and made available to the data subject (including the name of the notice and its location), the data subject voluntarily consents to the processing by the data controller of the personal data specified therein for the purposes and on the legal grounds set forth in the notice.

(13) [37]During the handling of a case, only those personal or special categories of data that are absolutely necessary for the case and for which the purpose-limitation principle can be demonstrated may be processed. The data may be used solely for the purpose of handling the specific case and, unless otherwise provided by law, may not be linked to other proceedings or data.

(14) [38]To ensure data quality, personal data may be recorded only from a valid official identification document suitable for identifying the data subject, and special categories of data may be recorded only with the data subject's written consent.

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

(16) [40]Personal and special categories of data recorded in paper-based notes that are not included in the case file must be rendered unidentifiable to prevent their further use. Working copies generated during computer processing, as well as corrupted copies or those that have become obsolete for other reasons, must be destroyed.

---

[33]REGULATION Article 32
[34]REGULATION Article 32
[35]REGULATION Article 6 paragraph (1)
[36]REGULATION Article 7
[37]REGULATION Article 5 paragraph (1) lit. b)
[38]REGULATION Article 5 paragraph (1) lit. d)
[39]REGULATION Article 5 paragraph (1) lit. d)
[40]REGULATION Article 5 paragraph (1) lit. f)

1.8. General Purposes of Data Processing, Data Processing Documents, and Records

Article 8

(1) [41]The University conducts data processing for administrative and record-keeping purposes based on different data processing objectives.

(2) The records and documents required by this Policy are maintained and prepared by the local data protection officer. The head of the organizational unit that designates the local data protection officer is responsible for the completeness of the records and for ensuring that the data contained therein are accurate and up-to-date.

1.9. Recording of Data Processing Activities

Article 9

(1) [42] At the University, the processing of personal data takes place following its entry into the data processing register in accordance with Article 30 of the Regulation.

(2) The University, as the data controller, maintains and preserves the data processing register in a decentralized manner through the local data protection officers.

(3) The head of the organizational unit managing the data file for registration purposes shall notify the ABK of the creation of a new data file prior to the commencement of the activity. If, in the course of their duties, the ABK or the data protection officer determines that the processing of personal data requires the maintenance of a register, they shall inform the head of the organizational unit and provide methodological assistance in performing the tasks related to the register.

(4) The data processing register must contain a record of data processing activities for all organizational units within the organizational unit, organized according to its internal structure. The organizational unit verifies the content and timeliness of the published registers through process-integrated self-monitoring, while the ABK conducts an annual audit. If necessary, the organizational unit supplements or amends the data processing register. In the event of discontinued data processing, the organizational unit archives the data processing register; in the event of new data processing, it establishes a new data processing register.

(5) Organizational units required to designate a local data protection officer shall publish the register on their websites in XLS format.

(6) A sample data processing record is available in the form library.

1.10. Data Transfer and Record-Keeping of Transferred Data

Article 10

(1) [43]Personal data may be transferred to persons other than the data subject only if such persons have expressly specified the purpose and legal basis of the data processing and are authorized by law to access the data.

[41]REGULATION Article 6
[42]REGULATION Article 30
[43] REGULATION Article 5 paragraph (2)

(2) Data transfers must be recorded in order to establish which data the data controller transferred, to whom, on what legal basis, and when, or which data was provided by (e.g., domestic legal assistance, etc.). If it is justified to enter a new entry into the register where the legal basis is unclear, the ABK will, upon a specific request from the local data protection officer, examine the legal basis and lawfulness of the data transfer and take a position on whether the data transfer can be carried out.
(3) The local data protection officer maintains the register on a per-organizational-unit basis.
(4) The head of the organizational unit is responsible to the data subject for the lawfulness of the data transfer with respect to the data processed by that unit.
(5) If the data transfer cannot be lawfully carried out, or if the data requester has not provided the information necessary to assess the request even after being prompted to do so, the data transfer must be denied.
(6) The requester must be notified in writing of the refusal to transfer the data, along with the reasons for the refusal.
(7) In proceedings initiated at the data subject's request, in the absence of statutory authorization for data transfer, the data subject must be asked—in writing with regard to special categories of data—whether they consent to the transfer of their personal data if contacting another authority is necessary to resolve their matter.
(8) The data subject has the right to request information regarding the processing of their personal data, as well as to request the correction of their personal data or—except in cases of mandatory data processing—their erasure or blocking. Requests for information regarding data processing must be fulfilled within a maximum of 30 days if the legal conditions are met; however, they should be processed on a priority basis whenever possible.
(9) Personal data may be transferred, disclosed, or combined with other data processing activities only if the data subject has consented to it, or if the law requires or permits it, and the conditions for data processing are met for each individual piece of personal data.
(10) The local data protection officer reviews the data transfer log by December 31 of each year, amends it if necessary, and prepares a report on the review. The report is sent electronically to the ABK by January 10 of the year following the year in question.
(11) The ABK shall publish in the form repository a template for the data transfer register prepared in accordance with Article 30 of the Regulation, as well as a template for the minutes required to conduct the review of the register.

1.11. Privacy Notices and Their Records

Article 11

(1) [44]If personal data concerning a data subject is collected from the data subject, the data controller shall inform the data subject by means of a privacy notice at the time the personal data is obtained; if the data was not collected from the data subject, the data controller shall inform the data subject within a reasonable period of time from the date the data was obtained, but no later than one month thereafter.

[44] REGULATION Articles 13 and 14

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

a) a general privacy notice summarizing the University's data processing activities (prepared by the Academic Board, issued by the rector, the chancellor, and the president of the Clinical Center),

b) specific data processing notices, which describe specific data processing activities defined for each individual purpose (prepared by: the local data protection officer; issued by: the head of the organizational unit required to designate a local data protection officer).

(3) [45]The general data processing notice includes:

a) the University's name and address,

b) the name and contact information of the University's representative,

c) the contact information of the University's data protection officer,

d) the purpose of processing the personal data handled by the University,

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

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

g) the main categories of data subjects,

h) the general processing and retention periods for data managed by the University,

i) the general organizational and technical measures implemented by the University to ensure data security,

j) any data protection incidents or risks that may occur during the University's data processing, and the measures taken to manage these risks,

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

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

(4) [46]General data processing notices by category of data subjects

a) on the processing of employee data,

b) the processing of student data,

c) the processing of health data,

d) data processing for research purposes,

e) data processing involving personal rights protected by specific laws.

(5) [47]In addition to the provisions set forth in paragraph (3) , the specific data processing notices include the purpose of processing

a) the purpose of processing the personal data processed for that specific purpose,

b) the legal basis for processing the data for that specific purpose,

c) the categories of personal data processed for that specific purpose,

d) the categories of data subjects affected by the processing for that specific purpose,

e) the general processing and retention periods for the data,

f) the general organizational and technical measures implemented to ensure data security,

g) any data protection incidents or risks that may occur during data processing for the specified purpose, and the measures taken to manage these risks,

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

h) the recipients of data transfers during data processing for the specified purpose,

i) the names and activities of joint controllers and data processors involved in the data processing for the specific purpose.

(6) [48]The University makes information about its data processing activities available to data subjects through data processing notices published on its website.

a) The ABK publishes the general data processing notices on the University's homepage.

b) Individual data processing notices must be posted on the homepage of the organizational unit required to designate a local data protection officer, and a link to these notices must be posted on the website of the Directorate-General for Legal and Administrative Affairs (hereinafter: JIF).

(7) [49]A record must be maintained of the publication of the specific data processing notices, containing the following information

a) the reference number of the privacy notice,

b) the title of the data processing notice,

c) the date of publication of the data processing notice,

d) the date the privacy notice expired or was amended.

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

(9) The ABK shall publish a template for the register, as well as a template for the minutes required to conduct the review of the register, in the form repository.

1.12. Disposal Register

Article 12

(1) [51]The local data protection officer shall provide information regarding the rights of the data subject as set forth in Articles 15–22 of the Policy

a) information,

b) access,

c) rectification,

d) restriction,

e) erasure/right to be forgotten,

f) data portability,

g) objection,

h) consent

— broken down by organizational unit — in a Record of Dispositions.

(2) The local data protection officer shall review the Record of Disposal by December 31 of each year, amend it as necessary, and prepare a report on the results of the review. The

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

report and its attachments shall be sent electronically to the ABK by January 10 of the year following the year in question.

(3) The ABK shall publish a template for the register, as well as a template for the minutes required to conduct the review of the register, in the form repository.

1.13. Registration of Data Processors, Joint Data Controllers, and Data Processing Activities

Article 13

(1) The ABK shall also review, within the framework of its legal advisory role, any data processing agreements entered into by the University with data processors, joint data controllers, or third-party data controllers.

(2) The ABK maintains a register of the contracts referred to in paragraph (1), which includes
   a) the name, address, and name of the representative of the data processor, joint data controller, or organization commissioning data processing;
   b) the name and contact information of the data protection officer of the data processor, joint data controller, or organization commissioning data processing;
   c) the purpose of data processing;
   d) the legal basis for processing the data processed for the purposes of data processing;
   e) the categories of personal data processed for the purposes of data processing;
   f) the categories of data subjects affected by the data processing;
   g) the scope of the agreement regarding data processing;
   h) the relevant organizational unit of the University.

(3) An agreement on data processing pursuant to Article 28 of the Regulation, and an agreement with joint controllers pursuant to Article 30 of the Regulation, must be concluded as an annex to the main contract. The ABK will publish a template for this in the form repository.

1.14. Data Protection Incidents and Their Recording

Article 14

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

(2) The local data protection officer shall report the detected incident in writing to the data protection officer and the information security officer no later than 36 hours after becoming aware of the incident.

(3) If this deadline is not met, the head of the relevant organizational unit shall prepare a report explaining the circumstances for the rector and the chancellor, who shall determine the next steps after consulting with the Data Protection Officer.

(4) [53]The University—through the Data Protection Officer—maintains a record for the purpose of monitoring measures related to the incident and informing the data subject; this record includes the scope of the personal data involved, the group and number of individuals

[52] REGULATION Article 33
[53] REGULATION Article 5 paragraph (2)

affected by the incident, the date, circumstances, and effects of the incident, the measures taken to address it, and any other information specified in the legislation governing data processing.

(5) [54]Within 48 hours of receiving the report, the Data Protection Officer shall decide whether the University is subject to a reporting obligation regarding the incident. If the University is required to report the incident to the data protection authority, the Data Protection Officer shall prepare the report for decision by the rector and the chancellor in such a way that the report can be submitted within 72 hours.

(6) [55]When assessing the risks of the incident, the data protection officer shall examine:
   a) the nature of the data protection incident,
   b) the scope and approximate number of data subjects affected,
   c) the categories and approximate number of data records affected by the incident,
   d) the name and contact information 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 address the incident, including, where applicable, measures to mitigate any adverse consequences resulting from the incident.

(7) The ABK publishes the forms required for reporting the incident to the data protection officer, assessing it, deciding on incident management, reporting it to the supervisory authority, and informing data subjects about the incident in the form repository.

(8) [56]The Data Protection Officer—in accordance with the decision of the rector and the chancellor—shall report the incident to the supervisory authority within 72 hours of becoming aware of it, if the data breach is likely to pose a risk to the rights of the data subject.

(9) [57]If the data breach is likely to pose a high risk to the rights and freedoms of the data subject, the University—in accordance with the Rector's decision—shall inform the data subject without undue delay, but no later than 30 days after becoming aware of the breach.

(10) The local data protection officer shall review the incident log maintained by him or her by December 31 of each year, make any necessary amendments, prepare a report on the results of the review, and submit it electronically to the ABK by January 10 of the year following the reporting year.

(11) The ABK shall publish the incident management record and the template for the report required to conduct the review of the record in the form repository.

1.15. Local Data Protection Officers and Their Registers

Article 15

(1) Pursuant to paragraph (2) of Article 3, the head of an organizational unit required to designate a local data protection officer must notify the ABK within 8 days of the designation or revocation of such an officer.

[54] REGULATION Article 33 paragraph (1)
[55] REGULATION Article 33 paragraph (3) Article 39 paragraph (19) lit. d)
[56] REGULATION Article 33 paragraph (1)
[57] REGULATION Article 34

(2) The ABK maintains a registry of local data protection officers.
(3) The registry contains:
a) the name of the organizational unit,
b) the name, position, and contact information of the local data protection officer,
c) the date of the local data protection officer's appointment or revocation.

2. Ensuring the rights of data subjects regarding data processing

2.1. Safeguarding the Rights of the Data Subject

Article 16

(1) The University facilitates the exercise of the data subject's rights. To exercise these rights, the data subject must verify their identity and eligibility when submitting a request. If the request is not submitted by an authorized person or if the requester cannot be identified, the request must be rejected. The request must be submitted using the form provided in the appendix to this Policy is freely available to anyone on the JIF website.
(2) The request may be submitted electronically to adatvedelem@semmelweis.hu or by mail to: Semmelweis University Data Protection and Patient Rights Center, P.O. Box 2, 1428 Budapest.
(3) If the request was submitted to another organizational unit of the University, it must be forwarded to the ABK within three business days.
(4) If the request is incomplete, the ABK will notify the applicant within 8 days to provide the missing information. The deadline for providing the missing information is not included in the 8-day forwarding period or the 30-day deadline for processing the request.
(5) The ABK will forward the application to the organizational unit responsible for processing it within 8 business days, along with its opinion on the applicant's eligibility and the feasibility of fulfilling the request.
(6) The head of the organizational unit shall inform the data subject of the measures taken in response to the request without undue delay, no later than 30 days from the date of receipt of the request.
(7) Taking into account the complexity of the request and the number of requests, the deadline may be extended by an additional two months if necessary. Both the ABK and the organizational unit involved in fulfilling the request are authorized to extend the deadline.
(8) The head of the organizational unit shall notify the data subject and, at the same time, the ABK of the extension of the deadline within one month of receiving the request, specifying the reason for the delay. If the data subject submitted the request electronically, the notification must be provided electronically whenever possible, unless the data subject requests otherwise.
(9) The head of the organizational unit reviewing the request shall notify the applicant in writing, stating the reasons, of the rejection of the request within one month of its receipt, and shall simultaneously notify the ABK.
(10) The local data protection officer shall maintain a record of the requests received and their fulfillment or rejection. The record shall include:
a) the case file number,

b) the applicant's identifying information,
c) the subject matter of the request and the type of right involved,
d) the date the request was received,
e) the fulfillment of the request and the date thereof,
f) the reason for and date of the request's rejection,
g) the duration of the review of the request.

2.2. Informing Data Subjects

Article 17

(1) [58]To ensure that data subjects are properly informed, the University issues a privacy notice regarding all of its data processing activities.
(2) In addition to the information recorded in the register of personal data processing, the privacy notice includes information stating that the data subject
a) has the right to obtain confirmation and information regarding the data processed about them,
b) how they may exercise their rights in connection with the processing of their data,
c) may request from the data controller access to, modification, correction, erasure, or restriction of the processing of personal data concerning them, and may object to the processing of such personal data,
d) request data portability from the data controller,
e) may withdraw their consent to data processing at any time, which does not affect the lawfulness of data processing carried out prior to the withdrawal based on such consent,
f) may lodge a complaint with the supervisory authority to protect their rights,
g) determine whether the provision of personal data is based on a legal requirement or a contractual obligation, or whether it is a prerequisite for entering into a contract,
h) whether you are required to provide the personal data, and what the possible consequences of failing to provide such data may be.
(3) In cases where data processing is based on a provision of law, the performance of a task carried out in the public interest or in the exercise of official authority, the fulfillment of a legal obligation applicable to the University, a contractual obligation, the legitimate interests of the University or a third party, or the legitimate interests of the data subject, the University shall provide this information electronically; The University makes the privacy notices available on its official website. The University informs data subjects of the location where the privacy notices are available for all instances of data processing.
(4) In cases of data processing based on the data subject's consent, the notice must be provided to the data subject—by hand delivery, postal delivery, or email—and a document confirming receipt must be retained alongside the data processing records. The information must be provided to the data subject prior to the collection of data from the data subject, in order to ensure transparent information, communication, and the implementation of

[58] REGULATION Article 15

appropriate measures for the exercise of the data subject's rights. If the data does not originate from the data subject, the data subject must be informed of this within 30 days.

(5) The head of the organizational unit required to designate a local data protection officer is responsible for providing this information.

2.3. Ensuring the Right to Modify and Correct Data

Article 18

(1) In exercising the right to rectification, the data subject has the right to have the University amend or correct personal data concerning him or her upon request and without undue delay. Taking into account the purpose of the data processing, the data subject has the right to request that incomplete personal data be supplemented, including, among other things, by means of a supplementary statement.

(2) Health data may only be amended or deleted in such a way that the originally recorded data remains legible.

(3) The head of the organizational unit responsible for data processing is accountable for correcting the data.

2.4. Ensuring the Right to Erasure

Article 19

(1) In ensuring the right to erasure, the data subject is entitled to have the University, upon request and without undue delay, examine whether

a) whether the processing of personal data is still necessary for the purpose for which it was collected or otherwise processed,

b) whether the data subject has withdrawn the consent on which the data processing is based, and whether there is another legal basis for the data processing,

c) whether the data subject has objected to the processing of their data and there is no overriding legitimate ground for the processing,

d) whether the data processing was carried out for direct marketing purposes and the data subject has objected to the processing,

e) whether the personal data was processed unlawfully,

f) whether the personal data must be erased to comply with a legal obligation under Union or Member State law applicable to the data controller,

g) whether the personal data was collected in connection with the offering of information society services.

(2) If the conditions for erasure of the data are met, the University will erase the data without undue delay in accordance with the data subject's request.

(3) If the processing of the data is required by law and authorized by law, the data controller shall inform the data subject of this fact at the same time as rejecting the request.

(4) The head of the organizational unit responsible for data processing is accountable for the erasure of the data.

2.5. Ensuring the Right to Restriction of Data Processing

Article 20

(1) In ensuring the right to restriction of data processing, the data subject is entitled to have the University restrict data processing without undue delay upon request in the following cases:
   a) if the data subject disputes the accuracy of the personal data, the restriction applies for a period enabling the data controller to verify the accuracy of the personal data,
   b) if the processing is unlawful and the data subject opposes the erasure of the data and has requested the restriction of its use instead,
   c) the data controller no longer needs the personal data for the purposes of processing, but the data subject requires it to establish, exercise, or defend legal claims;
   d) the data subject has objected to the processing; in this case, the restriction applies for as long as it remains to be determined whether the data controller's legitimate grounds take precedence over the data subject's legitimate grounds.

(2) The University—provided that the conditions for restricting data processing are met—shall act in accordance with the data subject's request without undue delay.

(3) The head of the organizational unit responsible for data processing is accountable for the restriction of data processing.

2.6. Ensuring the Right to Data Portability

Article 21

(1) In ensuring the right to data portability, the data subject has the right to request that the University, without undue delay, determine whether
   a) the processing is necessary for the performance of a contract to which the data subject is a party, or is necessary for taking steps at the data subject's request prior to entering into a contract, or
   b) the processing is based on the data subject's consent.

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

(3) The head of the organizational unit responsible for data processing is accountable for the transfer of data.

2.7. Ensuring the Right to Object to Data Processing

Article 22

(1) In exercising the right to object to data processing, the data subject has the right to request that the University, without undue delay, assess whether the right to object to data processing can be exercised, that is,
   a) whether the data processing was necessary for the performance of a task carried out in the public interest,

b) whether the data processing was necessary to safeguard the legitimate interests of the data controller or a third party.

(2) If the conditions for exercising the right to object to data processing are met and there is no other legal basis for processing the data, the University shall cease processing the data without delay in accordance with the relevant provision.

(3) The head of the organizational unit responsible for data processing is accountable for ceasing such processing.

2.8. Ensuring the Right of Access to Data

Article 23

(1) Based on the right of access to data, the data subject is entitled to receive information from the data controller regarding whether their personal data is being processed, and if such processing is taking place, they are entitled to access their personal data and the following information:

a) the categories of the data subject's personal data;

b) the purposes of the processing;

c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, including, in particular, recipients in third countries and international organizations;

d) the planned duration of the storage of the personal data, or, if this is not possible, the criteria used to determine that duration;

e) may request from the data controller the rectification, erasure, or restriction of processing of personal data concerning him or her, and may object to the processing of such personal data;

f) has the right to lodge a complaint with the supervisory authority;

g) if the data were not collected from the data subject, all available information regarding their source;

h) the fact of automated decision-making, including profiling, as referred to in Article 22 paragraphs (1) and (4) of the Policy as well as, at least in those cases, the logic applied and comprehensible information regarding the significance of such processing and the expected consequences for the data subject.

(2) If personal data is transferred to a third country or to an international organization, the data subject has the right to be informed about the appropriate safeguards regarding the transfer in accordance with Article 46 of the Regulation.

(3) The head of the organizational unit processing the data is responsible for ensuring the right of access to the data.

2.9. Review of the Legal Basis for Data Processing

Article 24

(1) [59]Each year, the University reviews the documentation for all personal data processing activities recorded in the data processing register to ensure that the data contained therein were processed in accordance with applicable laws and the University's regulations, that the appropriate legal basis for such processing continues to exist, and that the data in question are being processed on an appropriate legal basis. The head of the organizational unit shall act in accordance with the ABK's methodological guidelines regarding the legal basis for data processing.

(2) During the review of all data processing activities, the legal basis for data processing must be established, and it must be determined whether documentation supporting the legal basis necessary for data processing is available. If necessary, the ABK provides assistance in establishing the legal basis.

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

a) Data processing based on the data subject's consent: consent given by the data subject or their legal representative, which constitutes a voluntary and explicit expression of the data subject's will, based on adequate information (the purpose, legal basis, duration, the name and address of the data controller, the name and address of the data processor, and the activities related to data processing), and by which the data subject gives unambiguous consent to the processing of personal data concerning him or her—whether comprehensive or limited to specific operations;

b) Data processing necessary for the performance of a contract with the data subject or for the conclusion of a contract: the contract concluded with the data subject—a statement regarding the conclusion of the contract (specifying in the contract the necessary data processing, or set forth in a separate document indicating which provision of the contract the data processing is necessary to fulfill);

c) Data processing necessary to comply with a legal obligation to which the data controller is subject: the precise designation of the legal provision mandating or requiring the data processing;

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

da) what is the purpose of the data processing,

db) Is the processing of personal data strictly necessary to achieve the purpose of the data subject or another natural person?

dc) Are there alternative solutions available that would allow the intended purpose to be achieved without processing personal data?

dd) the most precise possible definition of the legitimate interest,

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

df) what interests the other party may have that lawfully justify data processing based on that party's interests;

[59] REGULATION Article 5 paragraph (1) lit. a), Article 6
[60]REGULATION Article 6

e) data processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller: the precise designation and text of the legal provision defining the public interest or the official authority vested in the data controller, as well as the necessity of the specific data processing as determined by such authority;

f) [61]necessary for the purposes of the data controller or a third party: whether a balancing test has been conducted,

fa) Is the processing of personal data absolutely to achieve the controller's or a third party's objective;

fb) are there alternative solutions available that would allow the intended purpose to be achieved without processing personal data,

fc) the most precise possible definition of the legitimate interest,

fd) what is the purpose of the data processing,

fe) what personal data the legitimate interest requires to be processed and for how long,

ff) what interests the other party may have that lawfully justify data processing based on that party's interests.

(4) [62]When documenting data processing based on consent, it is necessary to examine whether

a) whether documentation supporting the legal basis is available and whether it was lawfully obtained,

b) whether consent was the appropriate legal basis for processing the data,

c) whether the consent was given in an appropriate form,

d) whether the data subject received adequate information prior to giving consent.

(5) By making the form "REQUEST TO EXERCISE DATA SUBJECT RIGHTS," available for unrestricted download on its websites, the University ensures that data subjects have the right to withdraw, amend, or restrict their previous consent.

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

2.10. Processing of Special Categories of Data

Article 25

(1) The University processes special categories of personal data only if one of the conditions set forth in Article 9 paragraph (2) of the Policy is met.

(2) [63]When processing special categories of personal data, the local data protection officer shall verify, in every instance of data processing, whether the processing based on consent was carried out in accordance with data processing rules. The ABK's position statement serves as the guiding principle regarding the compliance of data processing with applicable laws.

[61] REGULATION Article 6 paragraph (1) lit. f), Preamble paragraph (69)
[62] REGULATION Article 7
[63] REGULATION Article 9

2.11. Ensuring the Prevention of Data Leaks

Article 26

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

(2) In accordance with the provisions of the Information Security Policy, the University takes the following measures to prevent the leakage of personal data:

a) it assesses the ongoing confidentiality, integrity, availability, and resilience of the systems and services used to process personal data,

b) assess the ability to restore access to personal data and the availability of such data in a timely manner in the event of a physical or technical incident,

c) establish a procedure for the regular testing, assessment, and evaluation of the effectiveness of the technical and organizational measures implemented to ensure the security of data processing within the framework of information security,

d) conducts a risk assessment to determine an appropriate level of security, to identify risks arising from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to personal data that is transmitted, stored, or otherwise processed, and to determine the potential harm resulting therefrom.

3. The University's Data Protection System

3.1. The Data Protection Officer

Article 27

(1) [65]The Chancellor, in consultation with the Rector, shall appoint an independent data protection officer from among the staff of the JIF who holds a law degree and has at least 3 years of experience in data protection — to perform the duties of a data protection officer for the University, both as a data controller and as a data processor.

(2) [66] The University shall ensure that the data protection officer can be appropriately and timely involved in all matters concerning the handling and processing of personal data. In order to perform their duties, the data protection officer is authorized to access data managed by the organizational units and to request data from them.

(3) The University shall provide the Data Protection Officer with the resources necessary to perform these duties, to access personal data and data processing operations, and to maintain the Data Protection Officer's expert-level knowledge.

(4) [67]The Data Protection Officer may not accept instructions from anyone regarding the performance of his or her duties. The Data Protection Officer is directly accountable to the University's senior management.

[64] REGULATION Article 32
[65] REGULATION Article 37 paragraph (5), paragraph (6)
[66] REGULATION Article 39
[67] REGULATION Article 38 paragraph (3)

(5) [68]The Data Protection Officer is bound by a duty of confidentiality in connection with these activities for an indefinite period, regardless of the duration of the employment relationship.

(6) The Data Protection Officer's duties include, in particular:

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

b) monitor, based on an annual work plan, the implementation of legal governance measures related to data protection and compliance with the rules, and report annually to the rector and the chancellor on these matters,

c) provides professional oversight of data protection training for staff,

d) provides professional advice upon request regarding data protection impact assessments and monitors the conduct of such assessments,

e) cooperates with the supervisory authority,

f) serves as the point of contact for the supervisory authority in matters related to data processing—including prior consultation—and consults with the supervisory authority on any other issues as appropriate,

g) contributes to the University's integrated risk assessment by identifying data protection risks,

h) as part of its advisory activities, makes recommendations on the topics for data protection training courses;

i) [69]assists data subjects in exercising their rights and initiates the necessary measures with the data controller to investigate and remedy complaints.

j) Based on information provided by the organizational units, the Data Protection Officer prepares an annual report for the Rector and the Chancellor evaluating the University's data protection activities by December 15 of each year—beginning in 2025—with the following content:

ja) the number and nature of data protection authority cases currently in progress or concluded during the year in question, along with the most important lessons learned;

jb) the number, nature, and key lessons learned from litigation cases involving data protection issues,

jc) progress on the data protection compliance project,

jd) a presentation of measures related to the organization of a network of local data protection officers,

je) a general assessment of the university's data protection activities.

jf) an overview of information related to the fulfillment of public interest data requests, including the nature and types of such requests, as well as compliance with deadlines.

(7) The Data Protection Officer is authorized to

a) to inspect all data processing activities falling under the scope of this policy and to enter any premises where data processing takes place,

[68] REGULATION Article 38 paragraph (5)
[69] REGULATION Article 38 paragraph (4), Information Act Article 25/M

b) request information and clarification regarding any data processing subject to this policy,

c) to participate, with the right to consult and approve, in any forum of the University and its organizational units where topics falling within his or her jurisdiction are on the agenda.

d) to issue data protection notices, data protection warnings, and data protection enforcement orders within its own jurisdiction, in accordance with Article 3 paragraph (4) lit. e) of Part I.1 of the University's Organizational and Operational Regulations;

e) initiate specific measures addressed to the rector, chancellor, or the president of the clinical center, proposing a managerial action if, based on the provisions of the normative regulatory document, it becomes necessary to take additional measures concerning a specific field, organizational unit, or employee(s) that fall outside the scope of the data protection officer's authority.

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

Article 28

(1) The ABK operates as an organizational unit of the JIF under the direction of the JIF's Director General and the professional supervision of the Data Protection Officer.

(2) The ABK is headed by the Director of Data Protection and Patient Rights.

(3) The ABK's responsibilities regarding regulations include:

a) regularly reviewing policies related to data processing and data security and ensuring they remain up to date,

b) preparing the forms specified in these policies and publishing them in the form repository,

c) participating in and providing professional advice to organizational units on the preparation and updating of the Articles of policies—including those containing rules related to data processing—that pertain to data processing.

(4) The ABK's advisory role:

a) [70]providing guidance and individual consultations to local data protection officers and organizational unit heads regarding the practical implementation of University procedures related to data protection and patient rights (data protection notices, patient information sheets, handling of complaints related to data processing, data disclosure, and record-keeping),

b) preparing methodological guidelines,

c) assisting the University's information security officer with data protection-related advice in licensing and approval procedures falling within the scope of their responsibilities.

(5) [71]The ABK is responsible for investigating complaints related to data processing in the context of complaint procedures.

(6) The ABK's role in oversight is as follows:

[70] Modified by: Senate Decision No. 31/2026 (March 25), Article 12. Effective from: April 1, 2026

[71] Modified by: Senate Decision No. 31/2026 (March 25), Article 12. Effective from: April 1, 2026

a) in the event of a report or detection of unauthorized data processing, it participates in the investigation and assists in remedying the situation,

b) it oversees the activities of organizational units and local data protection officers related to data protection tasks.

(7) The ABK's responsibilities in organizing training include:

a) developing training topics based on the recommendations of the data protection officer,

b) preparing data protection training materials for new employees based on the training curriculum,

c) organizing training for local data protection officers,

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

(8) The ABK participates in reviewing contracts related to data protection and the processing of personal data in accordance with the University's Contract Policy.

(9) ABK staff members are authorized, in the performance of their duties, to access data processed by organizational units and to request data from such units. ABK staff members are bound by a duty of confidentiality in connection with these activities, without any time limit and regardless of the duration of their employment relationship.

3.3. Appointment and Duties of the Local Data Protection Officer

Article 29

(1) The head of an organizational unit required to designate a local data protection officer is responsible for the data processing activities of the organizational unit(s) under his or her supervision.

(2) The head of an organizational unit required to appoint a local data protection officer

a) shall appoint the local data protection officer,

b) shall monitor the data protection officer's activities at regular intervals through reporting,

c) decide on the further storage or destruction of recorded data after the mandatory retention period has expired.

(3) The local data protection officer must be a person with professional competence and, in particular, expert-level knowledge of data protection law and practice, as well as the ability to perform the duties prescribed by law.

(4) The local data protection officer

a) shall ensure the preparation, maintenance, publication, and review of the organizational unit's records and privacy notices related to data processing, and shall inform the ABK of the results of the review in accordance with the provisions of this policy;

b) organizes data protection training for persons involved in data processing and data handling within the organizational unit,

c) upon request by the ABK, assists in responding to complaints regarding the processing of personal data by the organizational unit,

d) [72]upon request by the ABK, provides information regarding complaints related to data processing under its review, data requests, and the measures taken,

e) notifies the data protection officer of any suspected data protection incidents,

f) provides data to the JIF to respond to public interest data requests received by or available at the organizational unit.

(5) In the absence of a designated local data protection officer, the head of the organizational unit authorized to make such designations shall perform the duties of the local data protection officer as specified in this policy.

3.4. The Data Protection Oversight System

Article 30

(1) [73]The Rector, the Chancellor, and the President of the Clinical Center, through the Data Protection Officer and the ABK, monitor compliance with laws and regulations governing data processing and protection. By February 1 of each year, the Data Protection Officer prepares an annual report for the Rector, the Chancellor, and the President of the Clinical Center on the current status of data protection.

(2) The organizational units review their own data processing procedures and their compliance through self-assessments integrated into their processes.

(3) Local data protection officers shall review the records they maintain and the published data processing notices by December 31 of each year, and shall inform the ABK of the results of the review by January 10 of the year following the relevant year, in accordance with the provisions of this policy.

(4) The Data Protection Officer shall verify, based on an annual audit plan, whether the University's organizational units

a) are complying with their obligations regarding the protection of personal data, particularly

aa) the obligation to inform data subjects,

ab) their obligations regarding ensuring data subjects' right of access,

ac) their obligations regarding the protection of data subjects' rights.

b) whether they are complying with their obligations regarding data breaches,

(5) The data protection officer shall prepare a report on the audit and take the following measures:

a) if any deficiencies are identified, within 15 days, he or she shall call upon the head of the relevant organizational unit to take corrective action within a 15-day deadline,

b) after the deadline for taking action has passed, the Data Protection Officer shall conduct a follow-up inspection within 30 days to verify that the required action has been taken.

c) Within 15 days following the follow-up inspection, it verifies the implementation of the corrective action; if the action has not been taken or has been implemented inadequately, it notifies the Chancellor of the need for corrective action.

[72] Modified by: Senate Decision No. 31/2026 (March 25), Article 12. Effective from: April 1, 2026

[73] REGULATION, Article 39, Article 5 paragraph (2)

(6) The ABK reviews the annual review reports prepared by local data protection officers; in the event of deficiencies, it provides support through a staff member designated by the Director General for Legal and Administrative Affairs to ensure compliance.
(7) The Audit Directorate acts in accordance with the rules governing it during data protection-related investigations.

4. Supporting Compliance for the University's Data-Processing Units

Article 31

(1) The Director General of JIF has designated a staff member with independent responsibilities to promote data protection compliance. Working in cooperation with the local data protection officer of each organizational unit, this staff member provides methodological assistance to the organizational units in accordance with a schedule determined by the Director General of JIF—based on prior consultation with the Director of ABK—
   a) in preparing data protection documentation and maintaining it with appropriate content (data protection compliance audit),
   b) to assess the operational compliance of organizational units in accordance with the professional methodological requirements established by the data protection authority (data protection operational audit),
   c) to ensure data protection awareness as required by this Policy, based on the recommendations of the Data Protection Officer and, in accordance with the training curriculum established by the ABK, conducts data protection training and administers proficiency assessments for employees designated by the head of the organizational unit,
   d) regularly reports to the Director General of JIF on the latest developments regarding compliance support activities.

   e) The designated employee informs the relevant local data protection officer of his or her contact information and the training schedule.
(2) JIF publishes a methodological guide on its website
   a) on the processing of employee data,
   b) the processing of student data,
   c) the processing of health data,
   d) tasks related to the processing of data concerning personal rights protected by specific laws, as well as
   e) tasks related to supporting compliance with suitability and operational audits, and providing the training necessary to ensure data protection awareness,
   f) to promote data protection compliance for institutions under its jurisdiction
(3) Compliance with these guidelines is mandatory for individuals and organizations subject to the policy and is expected of institutions under the authority of the Ministry.

5. Data Protection Provisions Related to Scientific Research

Article 32

(1) Semmelweis University supports the independent and collaborative scientific research activities of members of the university community—in particular, but not exclusively, researchers, instructors, students, and doctoral students—(hereinafter: researchers)—to conduct independent and collaborative scientific research activities (hereinafter: scientific research); the University permits the access to and processing of data—including, where justified, data capable of identifying individuals—for the purposes of scientific research.

(2) If personal data is processed in the course of scientific research, the principal investigator is responsible for ensuring full compliance with the data protection and data security requirements set forth in applicable laws and the University's internal regulations.

(3) Personal data may be processed for scientific research purposes only on the basis of a research plan set forth in writing and approved in writing by the ethics committee (hereinafter: "research plan"), which has been approved by the principal investigator and the head of the organizational unit involved in the data processing. The organizational unit maintains a record of approved research projects.

(4) During the course of scientific research, the Researcher may process only data derived from verified sources that comply with professional and ethical standards, domestic and international laws, and the University's internal regulations (hereinafter: all regulations). The Researcher is responsible for verifying the source of the data.

(5) During scientific research, the Researcher may process personal data only
   a) with authorization in accordance with all regulations;
   b) for the purpose specified in the research plan and within the scope of data necessary to achieve that purpose;
   c) for the period necessary to achieve the objectives specified in the research plan;
   d) in a form separated from personally identifiable data through anonymization or pseudonymization procedures
   may be processed.

(6) During scientific research, no copies containing personal data may be made of the stored data.

(7) In the case of anonymization of personal data, the principal investigator is required to ensure that true anonymization is carried out in accordance with the law and to ensure that the anonymization is irreversible.

(8) In the case of pseudonymization of personal data, the principal investigator is required to ensure that genuine pseudonymization is carried out in accordance with the law. Additional information that would allow for the re-identification of natural persons may only be provided to the researcher if the legal basis for the scientific research is the data subject's informed consent, or if re-identification is carried out in a credible manner in the data subject's vital interest.

(9) The principal investigator is required to ensure that personal data used in the course of scientific research are not used for other research purposes, unless the legal basis for the scientific research is the data subject's informed consent.

(10) If personal data comes into a researcher's possession in a manner not regulated in connection with scientific research, the researcher shall block such data and immediately notify the principal investigator and the University's data protection officer.

(11) It is the responsibility of the principal investigator to establish an appropriate level of protection in connection with scientific research.

(12) When establishing these safeguards, efforts must be made to apply technical, organizational, programming, and legal measures, as well as tools that, based on the knowledge available to them, most effectively promote and ensure the protection of the subject matter against harmful effects and malicious intentions arising from various sources of risk.

(13) A researcher may participate in the processing of personal data during scientific research only if the principal investigator has provided training on the relevant professional, data protection, and data security rules.

(14) To conduct this training, the principal investigator may seek professional support from the Chief Information Officer and the University's Data Protection Officer regarding its content.

(15) It is the responsibility of the principal investigator to ensure that the researcher receives appropriate professional, data protection, and data security training prior to participating in scientific research—with particular regard to the pseudonymization and anonymization of data. The principal investigator shall maintain a record of the training provided and retain such record for 10 years.

(16) The principal investigator shall maintain a record of the training required under paragraph (13), which must include the following

a) the location of the training,

b) the name and signature of the person(s) conducting the training,

c) the topics covered during the training and key findings,

d) the names and signatures of the participants in the training.

(17) Data protection regulations must also be observed with regard to personal data obtained during scientific research, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The data protection principles set forth in the Regulation (GDPR)

a) the fundamental principles of data protection;

b) the rules governing data processing activities and the maintenance of records of individual data transfers;

c) provisions regarding the preparation and publication of a privacy notice; and

d) data security requirements.

(18) The Director General for Legal and Administrative Affairs shall provide methodological guidance on the record-keeping of data processing activities involving personal data used in scientific research.

(19) If the processing of personal data for the purposes of scientific research is carried out by a student or doctoral candidate of the University, the student's or doctoral candidate's advisor shall take the place of the research supervisor in the provisions of this Policy, and the specific provisions of the Academic and Examination Regulations and the Doctoral Regulations must also be applied during data processing.

(20) If the scientific research is based on international or domestic collaboration, the data protection agreement concluded between the parties involved in the research shall also govern data processing related to the research.

6. Final Provisions

Article 33

(1) The Senate of Semmelweis University, acting pursuant to the authorization granted in Article 19 (10) d) of Part I.1 of Book I of the Organizational and Operational Regulations, adopted the Regulations on Data Protection, Disclosure, and Requests for Data of Public Interest—Book I: Data Protection Regulations—by Resolution No. 88/2025. (September 25, 2025).

(2) Book I: Data Protection Regulations of the Regulations on Data Protection, Disclosure, and Requests for Information of Public Interest shall enter into force on October 2, 2025.

(3) Concurrent with the entry into force of these regulations, the Data Protection, Disclosure, and Public Interest Data Requests Regulations—Book I: Data Protection Policy, adopted by Senate Decision No. 107/2022 (December 19) and amended by Senate Decisions Nos. 118/2024 (December 16), 54/2023 (June 29), and No. 6/2025 (January 23), shall be repealed.

7. Appendices

Appendix 1: Types of records, data processing notices, and minutes maintained by the local data protection officer
Appendix No. 2: Audit Trail

1. Annex No. : Types of records, data processing notices, and minutes maintained by the local data protection officer

A) Data Processing Register—the register referred to in Article 30 of the Policy, which must be maintained according to the type of data processing activities:

1. professional activities
2. scientific research activities
3. labor and human resources activities
4. administrative activities (finance, secretariat, communications)

B) Data processing notices related to the data processing register

C) Additional registers:

1. Register of data processing notices
2. data transfer register
3. register of data subject consents
4. disposal register
5. training records
6. Data breach register

D) Minutes

1. Minutes on the required maintenance of records
2. self-inspection report

Appendix 2: Audit Trail

2/A. Data Protection and Patient Rights Center[74]

	Process Steps	Preparation Steps	Levels of Responsibility					Document Generated as a Result of the Process
			Task Owner	Auditor	Method of verification	Approver	Method of approval	
1.	Release of Patient Data	Assessment of the Feasibility of the Request	Designated ABK staff member	ABK Director	Document review, signature	ABK Director	Signature	response document
2.	Conducting an impact assessment	Assessing the need for new data processing, consultation with the data protection officer	Head of the relevant organizational unit, local data protection officer	Head of ABK, Data Protection Officer	Data analysis	ABK Director	Signature	document on the impact assessment
3.	Cooperation in the investigation of patient complaint handling at the request of the Legal Representation Directorate	Providing an opinion on submissions received from the Legal Representation Directorate to the	designated ABK staff member	ABK Director	Document review, signature	ABK Director	Signature	response document to the Litigation Directorate
4.	Handling of data protection complaints at the organizational level	Providing assistance and issuing a position statement on a specific matter upon request	Designated ABK staff member	ABK Director	Document review, signature	ABK Director	Signature	response document
5.	Preparation of guidelines	proposal to issue the guidelines	Designated ABK staff member	ABK Director	Document review, signature	ABK Director	Signature	guidance document
6.	Maintaining contact with	Scheduled and ad hoc meetings	ABK Director	n.e.	Document review, signature	ABK Director	Signature	Memos

[74] Modified by: Senate Decision No. 31/2026 (March 25), Article 12. Effective from: April 1, 2026

	Process Steps	Preparation Steps	Levels of Responsibility					Document Generated as a Result of the Process
			Task Owner	Auditor	Method of verification	Approver	Method of approval	
	patient rights representatives							
7.	Record-keeping	Development and ongoing implementation of records	Designated ABK staff member	ABK Director	Document review, signature	ABK Director	Signature	record with a signature certifying that the review was completed
8.	Review of contracts related to data protection and the processing of personal data	review of contracts	Designated ABK staff member	ABK Director	Document review, signature	ABK Director	Signature	draft contract compliant with data protection requirements
9.	Verification of the compliance of the university's data protection activities	Review of annual reports prepared by local data protection officers, ongoing activities throughout the year, and verification of the compliance of received documents	Designated ABK staff member	ABK Director	Reporting	ABK Director	Approval of the report	Report on the Results of the Compliance Review

2/B. Data Protection Officer

	Steps in the process	**Preparation steps**	**Levels of Responsibility**					**Document Generated as a Result of the Process**
			Task Owner	**Reviewer**	**Method of verification**	**Approver**	**Method of approval**	
1.	Information and advice	Reviewing the specific case, forming an opinion	Data Protection Officer	N/A	N/A	N/A	signature	Reply letter sent to the inquirer
2.	Monitoring the implementation of legal governance tools related to data protection	Planning and carrying out tasks outlined in the annual work plan	Data Protection Officer	N/A	N/A	N/A	signature	Annual Report to the Rector and Chancellor
3.	Audit of data processing activities	Performing tasks in accordance with the annual work plan	Data Protection Officer	N/A	Mid-year reporting	N/A	signature	Information for the Rector and Chancellor
4.	Handling Data Protection Incidents	Incident Detection, Assessment,	Local Data Protection Officer/Data Controller, Head of the Organizational Unit Affected by the Incident	Data Protection Officer	Analysis of data and information	Rector, Chancellor	signature	Incident response report, briefing for the rector and chancellor, and, if necessary, notification to the supervisory authority
5.	Maintaining contact and cooperating with the supervisory authority	collection and analysis of relevant information regarding the matter at hand, fulfillment of reporting obligations	Data Protection Officer	N/A	N/A	Rector, Chancellor	signature	report