# Foundation for National Health Care and Medical Education
# Privacy and Data Security Policy

*(codified as amended)*

**.....**

**Chairman of the Board of Trustees**

Adopted by the Board of Trustees on 23 September 2021, Resolution 19/2021 (IX.23.)
Amended by Board of Trustees Resolution 25/2022 (IX.5.), effective from 5 September 2022
Amended by Board of Trustees Resolution 40/2022 (XII.12.), effective from 1 January 2023

Table of contents:

1. GENERAL PROVISIONS ..... 4
*1.1. Scope of the Code* ..... *4*
*1.2. Principles, legal basis and purposes of data processing* ..... *4*
*1.3 Privacy by design, conduct a data protection impact assessment* ..... *6*
*1.4. Enforcing data protection principles and ensuring accountability* ..... *6*
*1.5. Data management and security requirements in the course of administration* ..... *7*
*1.6. General purposes of data processing, data management records* ..... *7*
*1.7. Records of processing activities* ..... *7*
*1.8. Transmission of data and recording of data transmitted* ..... *8*
*1.9. Information notices and record keeping* ..... *9*
*1.10. Register of Availability* ..... *10*
*1.11. Register of processors, joint controllers, data processing* ..... *10*
*1.12. Data protection incidents and their recording* ..... *10*
2. ENSURING THE RIGHTS OF DATA SUBJECTS WITH REGARD TO DATA PROCESSING ..... 11
*2.1. Safeguarding the rights of the data subject* ..... *11*
*2.2. Information to data subjects* ..... *12*
*2.3. Ensuring the right to modify and rectify data* ..... *13*
*2.4. Ensuring the right to erasure* ..... *13*
*2.5. Ensuring the right to restriction of processing* ..... *13*
*2.6. Ensuring the right to data portability* ..... *13*
*2.7. Ensuring the right to object to processing* ..... *14*
*2.8. Ensuring the right of access to data* ..... *14*
*2.9. Examination of the legal basis for processing* ..... *14*
*2.10. Processing of special data* ..... *15*
3. NEOA'S DATA PROTECTION REGIME ..... 16
*3.1. The NEOA Data Protection Officer* ..... *16*
*3.2. The control system* ..... *17*
4. PROCESSING FOR THE PURPOSE OF PROVIDING SUBSIDIES, DEBT COUNSELLING ..... 18
5. THE PROCESSING OF PERSONAL DATA OF THE MEMBERS OF THE BOARD OF TRUSTEES, THE MEMBERS OF THE SUPERVISORY BOARD, THE AUDITOR, PERSONS INVOLVED IN PERSONNEL MATTERS WITHIN THE SCOPE OF THE BOARD OF TRUSTEES' DECISIONS ..... 18
6. PROCESSING OF PERSONAL DATA RELATING TO ASSET MANAGEMENT ..... 19
7. PROCESSING OF DATA RELATED TO THE CONTROL OF MAINTENANCE AND OWNERSHIP ..... 19

8. PROCESSING OF PERSONAL DATA RELATING TO COMPLAINTS TO THE MAINTENANCE PROVIDER..... 19

*1. Annex 1: Audit trails* ..... ***Hiba! A könyvjelző nem létezik.***

*1. Processing of personal data* ..... ***Hiba! A könyvjelző nem létezik.***

*2. Data protection incidents* ..... ***Hiba! A könyvjelző nem létezik.***

*3. Data Protection Officer* ..... ***Hiba! A könyvjelző nem létezik.***

# 1. GENERAL PROVISIONS

## 1.1. Scope of the Code

(1) The scope of the Code covers

a) the Foundation for National Health Care and Medical Education (hereinafter NEOA) and all its data processing activities involving the processing of personal data;

b) to anyone who processes personal data or becomes aware of personal data in the course of NEOA's activities;

c) all data classified as private by the applicable legislation.

## 1.2. Principles, legal basis, and purposes of data processing

(1) Personal data must be processed under the following principles:

a) [1]legality, fairness, and transparency;

b) [2] goal orientation;

c) [3] data economy;

d) [4] Accuracy;

e) [5] limited shelf life;

f) [6] integrity and confidentiality.

(2) [7]As the controller, NEOA is responsible for compliance with data management principles and must demonstrate such compliance ("accountability").

(3) [8]NEOA will only process personal data if.

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

b) [9]processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into the contract;

c) [10]processing is necessary for compliance with a legal obligation to which the controller is subject;

d) [11]processing is required for the protection of the vital interests of the data subject or another natural person;

e) [12]processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller;

f) [13]necessary for the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms

[1] Article 5(1)(a) GDPR
[2]GDPR Article 5(1)(b)
[3]GDPR Article 5(1)(c)
[4]GDPR Article 5(1)(d)
[5]GDPR Article 5(1)(e)
[6]GDPR Article 5(1)(f)
[7]Article 5 (2) GDPR
[8]Article 6(1)(a) GDPR
[9] Article 6(1)(b) GDPR
[10]GDPR Article 6(1)(c)
[11]GDPR Article 6(1)(d)
[12]Article 6(1)(e) GDPR
[13]GDPR Article 6(1)(f)

of the data subject, which require the protection of personal data, mainly where the data subject is a child.

(4) Unique data can be processed if

a) [14]the data subject has given their explicit consent to the processing of the special categories of personal data for one or more specified purposes unless Union or Member State law provides that the data subject's consent cannot lift the general prohibition on processing special categories of personal data;

b) [15]processing is necessary for complying with the obligations of the controller or the data subject arising from legal provisions governing employment, social security, and social protection and for the exercise of their specific rights, where such processing is permitted by Union or Member State law or by collective agreements under national law providing adequate safeguards for the fundamental rights and interests of the data subject;

c) [16]processing is necessary for the protection of the vital interests of the data subject or of another natural person where the data subject is physically or legally incapacitated and is unable to give their consent;

d) [17]the processing is carried out in the context of the legitimate activities of a political, philosophical, religious, trade union, or other non-profit foundation, association, or any other non-profit organization, with appropriate safeguards, on condition that the processing relates solely to current or former members of such an organization or to persons who have regular contact with the organization concerning the purposes of the organization and that the personal data are not disclosed to persons outside the organization without the consent of the data subjects;

e) [18]processing for preventive health or occupational health purposes, where the Foundation has an employee, to assess the employee's ability to work, to make a medical diagnosis, to provide health or social care or treatment, or to manage health or social care systems and services, as required by EU or Member State law or under a contract with a health professional;

f) [19]the processing is necessary for reasons of public interest in the sphere of public health, such as the protection against serious cross-border threats to health or to ensure a high level of quality and safety of healthcare, medicines, and medical devices, and is based on Union or Member State law which provides for adequate and specific measures to safeguard the rights and freedoms of the data subject, in particular, professional secrecy;

g) [20]the 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 which is proportionate to the aim pursued, respects the essential content of the right to the protection of personal data and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject.

[14]Article 9(2)(a) GDPR
[15]GDPR Article 9(2)(b)
[16]GDPR Article 9(2)(c)
[17]GDPR Article 9(2)(d)
[18]GDPR Article 9(2)(h)
[19]Article 9(2)(i) GDPR
[20]Article 9(2)(j) GDPR

(5) [21]The data subject must be informed before the data are collected, the information based on which the data are processed with regard to Articles 13 and 14 of the GDPR. This information may take the form of the publication of a privacy notice.

(6) [22]Consent employing an explicit affirmative action, such as a written, including an electronic, or oral statement by the data subject, by which they freely, explicitly, informed, and unambiguously consent to process personal data concerning the natural person.

a) Consent covers all processing activities carried out for the same purpose or purposes.
b) In the case of processing for multiple purposes, consent must be given for each of the purposes for which the data are processed.

(7) The NEOA shall keep records of the consent given by the data subjects, containing the following information

a) the file number of the data processing consent
b) natural person identification data of the data subject
c) the name and number of the processing register
d) file number of the privacy notice
e) the date of approval for the processing
f) the date of withdrawal of consent

(8) [23]Persons who process personal data on behalf of NEOA must keep the personal data they obtain during their activities confidential without any time limit.

(9)

### 1.3. Data protection by design, data protection impact assessment

(1) [24]Before starting new processing operations (in particular when new processing technologies are used), if their nature, scope, context, and purposes are likely to result in a high risk to the rights and freedoms of natural persons, the NEOA will carry out a pre-processing impact assessment on the impact of the envisaged processing operations on the protection of personal data.

(2) The NEOA Data Protection Officer will give an opinion on the need to carry out an impact assessment and will decide, based on this opinion, whether an impact assessment should be carried out, which should not take longer than 30 days.

(3) The impact assessment covers the aspects set out in Article 35(7) of the GDPR.

(4) The NEOA will ensure its internal rules and procedures comply with data protection requirements. The opinion of the NEOA Data Protection Officer shall be sought before such policies and practices are issued.

### 1.4. Enforcing data protection principles and ensuring accountability

[21]Article 12 (1) GDPR
[22]GDPR Article 7
[23]Section 8 (4) of Act I of 2012, Section 25 of Act CLIV of 1997 on Health Care and Section 219 of Act C of 2012 on the Criminal Code
[24]Articles 25 and 35 GDPR

(1) [25][26] Accountability: the NEOA will record its compliance review with the principles and, if necessary, propose changes, additions, deletions, deletions, or additions to documents and data. NEOA's Data Protection Officer will comment on the proposals by 15 March each year and send their opinion to NEOA, which will make the necessary changes by 31 May each year.

(2) NEOA officers and staff are directly responsible for data processing, personal data protection, and the lawfulness of data processing. The NEOA Data Protection Officer will support the activities related to protecting personal data, providing guidance where necessary, either on a specific or general basis.

### 1.5. Data management and security standards in the course of administration

(1) [27]For each record, access rights should be defined per person. This task must be completed within 30 days of the new employee's employment date if the Foundation has an employee or within 30 days if the employee's job title changes.

(2) The NEOA keeps a record of the entitlements.

(3) [28]Only personal or specific data which are indispensable for the management of the case and the purpose of which can be justified should be collected and processed. The data collected may only be used for the matter in question and may not be linked to other procedures and data unless otherwise provided by law.

### 1.6. General purposes of data processing, data management records

(1) [29]NEOA processes data for administrative and record-keeping purposes.

(2) The records and documents required by this Code (register of data processing, information notes and their registration, register of data transfers, register of the exercise of data subjects' rights, records of the review of processing and their registration) shall be drawn up and kept by the person designated by the NEOA.

### 1.7. Records of processing activities

(1) [30]The person who maintains and is designated to maintain a record for record-keeping purposes shall notify the NEOA Data Protection Officer of creating a new record 60 days before the start of the activity.

(2) At NEOA, the processing of personal data takes place after the registration in the Data Processing Register; the Data Processing Register (hereinafter referred to as the "RTR") contains the data pursuant to Article 30 of the GDPR.

[25] Articles 5(2), 5(1) and 6 of the GDPR
[26]Article 5(2) GDPR.
[27]Article 32 GDPR
[28]GDPR Article 5(1)(b)
[29]GDPR Article 6
[30]Article 30 GDPR

(3) The person responsible for the preparation is the data controller designated for this purpose. The Data Protection Officer of NEOA checks the adequacy of the content of the SADs and their up-to-dateness through an annual audit and, if necessary, supplements and amends the SADs. In the case of discontinued data processing, the SAD shall be archived, and in the case of new data processing, a new SAD shall be drawn up. The NEOA Data Protection Officer will provide methodological assistance to complete the PAD.
(4) The designated person who carries out the processing shall keep one copy of the DPA, and the NEOA Data Protection Officer shall keep a second copy.
(5) NEOA's Data Protection Officer maintains NEOA's aggregated data management records with aggregated data content based on the ANY tabs.

### 1.8. Transmission of data and record of data transmitted

(1) [31]The personal data shall be transmitted to persons other than the data subject who have explicitly indicated the purpose and legal basis for the processing and are authorized by law to access the data.
(2) Data transfers must be recorded to establish which data have been transferred or provided by the controller, to whom, based on what authorization, and when (e.g., domestic legal assistance, etc.) The data to be recorded are the identity of the data subject, the scope of the data transferred, the legal basis for the transfer, the addressee of the data transmitted, and the date of the transfer.
(3) The person designated by the NEOA keeps the register. A copy of the record shall be sent to the NEOA Data Protection Officer by 31 January following the end of the year in question. The register of transfers shall be kept for at least five years in the case of personal data and at least 20 years in the case of sensitive data unless otherwise provided by law.
(4) The records shall be kept with the following data content:
   a) file number
   b) details of the applicant
   c) type of data requested
   d) title of the data request
   e) date of application concerned
   f) date of completion
   g) date of refusal
   h) reason for refusal
   i) reason for partial fulfillment.
(5) Any refusal to transfer data shall be notified in writing to the applicant and the reasons for the denial.
(6) Personal data may only be transferred or supplied, and different processing operations may only be combined if the data subject has given their consent or if required or permitted by law and the conditions for processing are fulfilled for each personal data subject.

[31] GDPR (Article 5(2)).

### 1.9. Information notices and their recording

(1) [32]If personal data relating to the data subject are collected from the data subject, the controller shall inform the data subject by employing a privacy notice at the time of obtaining the personal data or, if not collected from the data subject, within a reasonable period from the date of receiving the data, but no later than one month.

(2) The NEOA shall publish the individual data processing notices as a description of the particular processing activities, delimited according to the purposes of each processing operation, with the content referred to in paragraph 3. The content of the privacy notices shall be subject to the opinion of the NEOA Data Protection Officer and the approval of the Chair of the NEOA Board of Trustees.

(3) [33]The General Data Protection Notice contains the following:

a) the name and address of the NEOA,
b) the name and contact details of the NEOA representative,
c) the contact details of the NEOA Data Protection Officer,
d) the purpose of the processing of personal data by NEOA,
e) the legal basis for the processing of data by NEOA;
f) the main categories of personal data processed by NEOA,
g) the main types of persons concerned by the NEOA's processing,
h) the general handling and retention period of the data processed by NEOA,
i) the general organizational and technical measures taken by NEOA to ensure data security,
j) any data breaches that may occur in the course of NEOA's processing, the risks involved, and the measures taken to address those risks,
k) the recipients of the personal data service regularly provided by NEOA,
l) the category of joint controllers and processors used in the NEOA's data processing activities and the nature of their activities,
m) the general organizational and technical measures taken by NEOA in the interest of data security,
n) the data protection incidents and risks that may occur in the course of NEOA's processing of data in the relevant sector and the measures taken to address these risks,
o) the names and activities of the joint controllers and processors used by NEOA for the processing of data in the given sector,
p) the recipients of the personal data services regularly provided by NEOA.

(4) [34]The NEOA delivers information on its data management activities to the data subject by publishing information notices on its website.

a) The privacy notice should be placed on the NEOA website

(5) [35]A record of the publication of specific privacy notices shall be kept with the following content

a) the number of the privacy notice,
b) the title of the privacy notice,
c) the date of publication of the privacy notice,
d) the date of publication of the privacy notice,

[32] Articles 13 and 14 GDPR
[33] GDPR Article 13
[34] Article 5(2) GDPR.
[35] Article 5(2) GDPR.

e) the date of expiry/amendment of the privacy notice.

(6)

(7) The Data Protection Officer of NEOA will publish a model register of privacy and privacy notices and a model protocol for reviewing the record.

### 1.10. Register of registrations

(1) [36]The NEOA keeps a record of the fulfillment of the data subject's rights as set out in Articles 15-22 of the GDPR (the "Register of Processing").

(2) The register shall contain

a) the date of the data subject's request,

b) the date of the response to the request,

c) the date of execution/rejection,

d) the grounds for refusal.

(3) [37] Unless otherwise provided by law, the records of transfers must be kept for at least five years for personal data and at least 20 years for sensitive data.

(4) A sample of the form and content of the Register of Administrations and an example of the record required for the review of the Register will be published by the NEOA Data Protection Officer.

### 1.11. Register of processors, joint controllers, data processing

(1) [38]NEOA's Data Protection Officer keeps records of data processors under contract with NEOA and data controllers processing data jointly with NEOA and of data processing carried out by NEOA for third-party data controllers, as defined in the GDPR and the Data Protection Act.

(2) The register shall contain

a) the name, address, and representative of the data processor, joint controller, data controller, data processor, or data controller;

b) the name and contact details of the data protection officer of the data processor, joint controller or data controller, or data controller organization;

c) the purpose of the processing;

d) the legal basis for the processing of data for data processing/processing;

e) the categories of personal data processed for the processing;

f) the categories of persons concerned by the processing for the processing;

the scope of the data processing agreement.

### 1.12. Data protection incidents and their recording

(1) [39]Employees are required to report a data breach to the Data Protection Officer within 24 hours of becoming aware of it.

[36] Article 5(2) GDPR.
[37] Article 5(2) GDPR.
[38] Articles 26 and 28, Article 5(2) GDPR.
[39] Article 33 GDPR

(2) [40]NEOA shall, through the NEOA Data Protection Officer, keep a record of the personal data concerned, the number and type of data subjects affected by the data breach, the date, circumstances, effects, and measures taken to remedy the data breach, and other data specified in the legislation requiring the processing, to monitor the actions taken concerning the data breach and inform the data subject.

(3) [41]Within 48 hours of the notification, the NEOA Data Protection Officer will decide whether the NEOA has a reporting obligation concerning the data breach. If NEOA is required to report, the NEOA Privacy Officer shall prepare the report for decision by the NEOA Board of Trustees Chairperson so that the report can be made within 72 hours.

(4) [42]When analyzing the risk of an incident, it is reviewed by the NEOA Data Protection Officer:

a) the nature of the data breach,
b) the scope and approximate number of persons concerned,
c) the categories and approximate number of data affected by the incident,
d) the name and contact details of the Data Protection Officer or another contact person who can provide further information,
e) the likely consequences of a data breach,
f) the measures taken or envisaged to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse effects of the personal data breach.

(5) [43]The NEOA Data Protection Officer shall, as decided by the Chair of the NEOA Board of Trustees, notify the supervisory authority of the occurrence of an incident if the incident is likely to pose a risk to the rights of the data subject within 72 hours of becoming aware of it.

(6) [44]If the personal data breach is expected to result in a high risk to the rights and freedoms of the data subject, the NEOA shall, without undue delay and within a maximum of 30 days, inform the data subject of the personal data breach.

## 2. ENSURE THE RIGHTS OF DATA SUBJECTS CONCERNING DATA PROCESSING

### 2.1. Ensuring the rights of the data subject

(1) The data controller may refuse to comply with a request to exercise the rights of the data subject only if the data controller proves that it cannot identify the data subject based on the available data.

(2) The controller shall inform the data subject of the action taken on the request without undue delay and, in any event, within one month of receipt of the request. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The NEOA Data Protection Officer is authorized to extend the time limit.

[40] GDPR Article 5 (2) para.
[41] Article 33 (1) GDPR.
[42] Article 33(3) GDPR. Article 39 (19) (d)
[43] Article 33 (1) GDPR.
[44] Article 34 GDPR

(3) The NEOA Data Protection Officer will inform the applicant in writing of the refusal of the request, stating the reasons for the denial, within one month of receipt of the request.
(4) The NEOA Data Protection Officer will keep a record of the requests received and whether they have been fulfilled or rejected. The records include the following:
   a) the file number
   b) identification details of the applicant
   c) the subject of the request and the right concerned
   d) the date of receipt of the request
   e) the date and time of the request
   f) the reason and date for the refusal of the request
   g) the period needed to process the application.
(5) If the controller fails to act on the data subject's request, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the possibility for the data subject to lodge a complaint with a supervisory authority and to exercise their right of judicial remedy.
(6) The data subject may submit the request to the NEOA Data Protection Officer electronically or on paper by post to the following postal address: the Data Protection Officer of the National Foundation for Health and Medical Education 1085 Budapest, Üllői út 26. or 1428 Budapest, Pf.2.

### 2.2. Information to data subjects

(1) [45]NEOA publishes a privacy notice on all its data processing to ensure that data subjects are adequately informed. The information notice issued by NEOA shall be easily accessible and written in plain, clear, and simple language.
(2) Additionally, to what is set out in the register on the processing of personal data, the privacy notice contains information on the following:
   a) the data subject has the right to obtain confirmation and information about the data processed concerning them,
   b) how the data subject may exercise their rights concerning the processing.
   c) the data subject may request the controller to access, amend, rectify, erase, or restrict the processing of personal data relating to them and may object to the processing of such personal data,
   d) may request the portability of the data subject's data from the controller,
   e) the data subject may withdraw their consent to the processing at any time, without prejudice to the lawfulness of the processing carried out based on the consent before its withdrawal,
   f) may lodge a complaint with the supervisory authority to protect the rights of the data subject,
   g) whether the provision of personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract,
   h) whether the data subject is obliged to provide the personal data and the possible consequences of not providing the data.
(3) In the case of processing according to a legal provision, the performance of a task carried out in the exercise of official authority or the public interest, the fulfillment of a legal obligation to which the controller is subject, a contractual duty or a legitimate interest of

[45] Article 15 GDPR

the controller or a third party, or in the interest of the data subject, the NEOA shall provide the information electronically; the information notices shall be made available on the NEOA website. The NEOA shall inform the data subjects of the location of the availability of the information notice for all processing operations.

### 2.3. Ensuring the right to modify and rectify data

(1) [46]The NEOA ensures that the data subject can exercise their rights to modify and rectify their data in a non-biased manner based on appropriate information.
(2) In granting the right of rectification, the data subject shall have the right to obtain, upon request, the rectification or correction of personal data concerning them by NEOA without undue delay. Considering the purpose of the processing, the data subject shall have the right to request the completion of incomplete personal data, including utilizing a supplementary declaration.

### 2.4. Ensuring the right to erasure

(1) [47]The NEOA ensures that the data subject can exercise their right to erasure based on adequate information and free from any influence.
(2) In granting the right to erasure, the data subject is entitled to have NEOA examine, at their request and without undue delay, whether any of the grounds set out in the GDPR apply.
(3) If the data processing is required or authorized by law, the controller shall inform the data subject of this at the same time as the request is refused.

### 2.5. Ensuring the right to restriction of processing

(1) [48]The NEOA ensures that the data subject can exercise their rights to restrict processing based on adequate information and free from any influence.
(2) In granting the right to restriction of processing, the data subject is entitled to have the NEOA restrict processing without undue delay at their request if the conditions of the GDPR are met.
(3) NEOA shall, where the conditions for the restriction of processing exist, without undue delay, provide for their limitation per the data subject's request.

### 2.6. Ensuring the right to data portability

(1) [49]The NEOA ensures that the data subject can exercise their rights to data portability based on appropriate information and free from any influence.
(2) In ensuring the right to data portability, the data subject shall have the right to have the NEOA examine, at their request and without undue delay, whether.

[46] Article 16 GDPR
[47] Article 17 GDPR
[48] Article 18 GDPR
[49] Article 20 GDPR

a) Processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into the contract; or
b) is based on the consent of the data subject

and the processing is carried out by automated means.

(3) If the conditions for the data portability are met, the NEOA shall, without undue delay and per the data subject's request.
a) Provide the data in a structured, commonly used, machine-readable format,
b) transfers the data directly to the controller designated by the data subject.

### 2.7. Ensuring the right to object to processing

(1) [50]The NEOA ensures that the data subject can exercise their right to object to processing based on adequate information and free from any influence.
(2) When the right to object to processing is granted, the data subject is entitled to have the NEOA examine, at their request and without undue delay, whether the right to object to processing is enforceable under the GDPR.
(3) If the conditions for exercising the right to object to processing are met, and there is no other legal basis for processing the data, NEOA shall, per the data subject's instructions, cease processing the data without delay.

### 2.8. Ensuring the right of access to data

(1) [51]The NEOA ensures that data subjects can exercise their proper access to data in an informed and non-discriminatory manner.
(2) Based on the data access right, the data subject has the right to obtain from the controller feedback as to whether or not their data are being processed and, if such processing is taking place, the right to access the personal data and information about their processing as provided for in the GDPR.
(3) Where personal data are transferred to a third country or an international organization, the data subject is entitled to be informed of the appropriate safeguards for the transfer under Article 46 of the GDPR.

### 2.9. Examination of the legal basis for processing

(1) [52]NEOA continuously examines the documentation of all personal data processing recorded in the data management register to ensure that the data contained therein are processed under the law and NEOA's policies, that the legal basis for the processing is valid, and that the data processing is based on the appropriate regulations. The opinion of the NEOA Data Protection Officer shall be the determining factor in determining the legal basis for the processing.

[50]GDPR Article 21, Article 22
[51]Article 15 GDPR
[52] GDPR Article 5(1)(a), Article 6

(2) When examining the processing of any data, the legal basis for the processing and the existence of documentation supporting the legal basis for the processing must be established.

(3) [53]To document the processing based on consent, NEOA should review, for each processing based on consent, whether

a) the documentation supporting the legal basis is available and has been obtained following internal procedures,
b) whether consent was the appropriate legal basis for processing the data,
c) whether the consent was given in the correct format,
d) whether the data subject has received pertinent information before giving consent.

(4) By making the statement available on its websites for download without restriction, NEOA ensures the right of the data subject of data processing based on consent to withdraw, modify or restrict the consent statement.

### 2.10. Special data management

(1) [54]In the case of processing special categories of personal data, NEOA must verify in each processing operation whether the processing based on consent or particular types of personal data has been carried out per the processing rules. The opinion of the NEOA Data Protection Officer shall be the relevant authority for complying with the processing operation with the law.

(2) The NEOA will examine whether the processing of the special categories of data it handles has been carried out under one of the following authorizations:

a) The data subject has given their explicit consent to the processing of those personal data for one or more specified purposes, and Union or Member State law does not provide that the data subject's consent cannot lift the prohibition,
b) processing is necessary for compliance with the obligations of the controller or the data subject arising from legal provisions governing employment and social security and social protection and for the exercise of their specific rights, where such processing is permitted by Union or Member State law or by collective agreements under national law providing adequate safeguards for the fundamental rights and interests of the data subject,
c) processing is necessary for the protection of the vital interests of the data subject or of another natural person where the data subject is physically or legally incapacitated and is unable to give their consent,
d) the processing is carried out in the context of the legitimate activities of a foundation, association, or any other non-profit organization with a political, philosophical, religious, or trade union aim, with appropriate safeguards, on condition that the processing relates solely to current or former members of such an organization or to persons who have regular contact with the organization concerning the purposes of the organization and that the personal data are not disclosed to persons outside the organization without the consent of the data subjects,
e) the processing relates to personal data which have been explicitly made public by the data subject,

[53] GDPR Article 7
[54] GDPR Article 9

f) processing is necessary for the establishment, exercise, or defense of legal claims or when the courts are acting in their judicial role,
g) processing is required for a substantial public interest based on Union or Member State law, which is proportionate to the aim pursued, respects the essential content of the right to the protection of personal data, and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject,
h) processing for preventive health or occupational health purposes, where the Foundation has an employee, to assess the employee's ability to work, to make a medical diagnosis, to provide health or social care or treatment, or to manage health or social care systems and services, as required by EU or Member State law or under a contract with a health professional,
i) the processing is necessary for reasons of public interest in the area of public health, such as the protection against serious cross-border threats to health or to ensure a high level of quality and safety of healthcare, medicines, and medical devices, and is based on Union or Member State law which provides for adequate and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy,
j) the 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 which is proportionate to the aim pursued, respects the essential content of the right to the protection of personal data and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject.

## 3. THE NEOA DATA PROTECTION SCHEME

### 3.1. NEOA Data Protection Officer

(1) [55],[56] The Chair of the NEOA Board of Trustees appoints an independent Data Protection Officer (hereinafter referred to as the NEOA Data Protection Officer), who has a degree in law or health care and at least three years of experience in data protection, to act as the NEOA's Data Protection Officer as the data controller or data processor, as decided by the NEOA Board of Trustees.

(2) [57]The NEOA Data Protection Officer's duties include in particular:
   a) Provide information and technical advice to the controller or processor,
   b) Monitors the implementation of the legal governance tools for data protection and compliance with the rules based on an annual work plan, reporting annually to the NEOA Board of Trustees Chair and the NEOA Board of Trustees Chair,
   c) professionally supervises staff training on data protection,
   d) on request, provide technical advice on the data protection impact assessment, and monitor the implementation of the impact assessment,
   e) cooperate with the supervisory authority and,

[55] Article 37 (5), (6) GDPR.

[57] Article 39 GDPR

f) act as a contact point for the supervisory authority on matters relating to data processing, including prior consultation, and consult it on any other matter as appropriate,
g) contribute to the NEOA's integrated risk assessment to identify data protection risks,
h) as part of its advisory role, it proposes topics for training on data protection.
i) [58]Assists the data subject in exercising their rights, investigates the data subject's complaint, and initiates the necessary measures to remedy the complaint.
j) Cooperate with the University's Data Protection Officer.

(3) The NEOA Data Protection Officer is entitled to.
a) Inspect all processing covered by this Policy and enter any premises where processing occurs,
b) request information and clarification on any processing covered by this Policy,
c) and participate with deliberation rights and approval in all fora where matters within its remit are on the agenda.

(4) The controller and the processor shall ensure that the NEOA Data Protection Officer has appropriate and timely access to all issues relating to personal data protection. They shall have the right to access the data processed to perform their tasks.

(5) [59]The NEOA Data Protection Officer may not accept instructions from anyone concerning performing their duties.

(6) [60]The NEOA Data Protection Officer shall not hold any position within NEOA that is incompatible with their assignments.

(7) [61]The DPO is bound by confidentiality obligations in the context of their activities, regardless of the duration of the legal relationship and without any time limit.

### 3.2. The control system

(1) [62]The Chair of the NEOA Board of Trustees, through the NEOA Data Protection Officer, will review compliance with the obligations related to the implementation of data management and protection legislation in a process-oriented manner. The NEOA Data Protection Officer shall report annually to the NEOA Board of Trustees Chair on the review results**.**

(2) The data controllers examine the data management processes and their compliance by employing self-auditing built into the process.

(3) NEOA's Data Protection Officer will monitor the compliance of data processing activities with this Policy.

(4) A report of the inspection is drawn up, and the following measures are taken:
a) where a deficiency is detected within 15 days, and with a deadline of 15 days, invite the person concerned to take action,
b) will conduct a follow-up inspection within 15 days of the deadline to verify compliance with the move.
c) Within eight days of the follow-up audit, it checks the implementation of the action, informs the NEOA Board of Trustees Chair if the action is not taken or not

[58] GDPR Article 38 (4) para., Infotv. § 25/M
[59] Article 38(3) GDPR.
[60] Article 38(6) GDPR.
[61] Article 38 (5) GDPR
[62] Article 39, Article 5(2) GDPR.

adequately implemented, and requests action to remedy the deficiencies by issuing an action plan within 15 days. If the action is not taken, the NEOA shall inform the Chairman of the NEOA Board of Trustees of the deficiency and the failure to take action within 15 days.

## 4. THE PROVISION OF SUBSIDIES, PROCESSING FOR DEBT COUNSELLING PURPOSES

(1) If NEOA operates a subsidy program for implementing public tasks, it processes the personal data of participants in these programs to award and account for subsidies.

(2) NEOA processes the applicants' personal data for awarding and accounting for the provision of means-tested grants for the performance of public tasks.

(3) NEOA processes the personal data of participants in talent management programs to award and account for implementing public tasks in the case of talent management programs.

(4) [63]Special categories of personal data are processed by processing data necessary for the assessment of special treatment of persons with disabilities, which may take place based on the explicit, freely given consent of the data subject.

(5) [64]Where the processing of personal data is not governed by the law of a Member State and other legal bases provided for by the legislation referred to do not apply, personal data may only be processed based on the data subject's consent. Such processing includes, for example, the provision of contact details, the submission of a curriculum vitae, the completion and submission of a leisure activity form, other processing related to the fulfillment of studies, and the recording of the results of a study competition or a contest.

## 5. THE PROCESSING OF PERSONAL DATA OF MEMBERS OF THE BOARD OF TRUSTEES, MEMBERS OF THE SUPERVISORY BOARD, THE AUDITOR, PERSONS INVOLVED IN PERSONNEL MATTERS WITHIN THE SCOPE OF THE BOARD OF TRUSTEES' DECISIONS

(1) Under the KEKVA Act and its operational rules as defined in its Statutes to fulfill its public tasks, NEOA processes the personal data of the members of the Supervisory Board and the Auditor necessary for the mandate and dismissal of the members of the Supervisory Board, including, where applicable, the personal data required for the fulfillment of the qualification requirements.

(2) NEOA processes the personal data of the members of the Supervisory Board and the Auditor necessary for the communication and functioning of the Supervisory Board, including the personal data (image, sound) essential for electronic communication, to fulfill its public tasks as defined in the KEKVA Act and its operational rules as defined in its Statutes.

(3) The NEOA processes the personal data of the persons (Rector, Chancellor) involved in personnel matters within the scope of the Board of Trustees' decisions to fulfill its public tasks as defined in the KEKVA Act.

[63] GDPR Article 6 (1) c.), a.)
[64]GDPR Article 6 (1) a.)

## 6. PROCESSING OF PERSONAL DATA RELATING TO THE MANAGEMENT OF ASSETS

NEOA's public task, as defined in the KEKVA Act, is to process personal data contained in contracts and grant agreements (including grants given and received by NEOA) relating to using its assets to fulfill the Board of Trustees' tasks of asset management and administration.

## 7. PROCESSING OF DATA RELATED TO THE CONTROL OF MAINTENANCE, OWNERSHIP

To fulfill its public task defined in the KEKVA Act, NEOA processes the personal data necessary for the owner's decisions and controls, including the personal data required for the exercise of these powers, to fulfill the control tasks of the Board of Trustees arising from the maintenance and ownership powers of the institution under its maintenance, NEOA is an independent data controller concerning these data.

## 8. THE PROCESSING OF PERSONAL DATA RELATING TO COMPLAINTS LODGED WITH THE MAINTENANCE PROVIDER

(1) In investigating complaints submitted to the NEOA, the NEOA will process the complainant's data to the extent necessary and proportionate for the investigation of the complaint.
(2) NEOA will process the contact details of the complainant separately from the other personal data of the complainant and will only process those data in an anonymized form, the anonymized data will only be accessible by the institution it is maintained by, and thus NEOA will not process personal data other than the contact details.

Annexes: Annex 1: Audit trails