Approval

	Name	Position	Signature	Date
Created by:	Viktória Papp	DPO		2023/aug./29
Reviewed by:	Zseni Anna	Legal Counsel		2023/Aug/29
Approved by:	Balázs Alpár	Quality Engineer		2023/Sep/01
Approved by:	Tamás Gyurkovics	CEO		2023/Aug/29

Release

	Name	Position	Signature	Date
Released by:	István Hajdu	Quality Engineer		2023/Sep/01

Revision history

Version	Date of initiation	Created by	Reason of change	Description of change
01	2021/SEP/01	Viktória PAPP	Initial version	
02	2023/JUL/15	Viktória PAPP	No English version of the document is available.	English version is created.

Table of Contents

INTERNAL DATA PROTECTION AND DATA SECURITY POLICY

The Neunos Zrt. (“Company”) establishes the following Internal Data Protection and Data Security Policy (“Policy”) based on the Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Infotv."), the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data - repealing Directive 95/46/EC (General Data Protection Regulation, "GDPR") and with regard to health data based on the Act XLVII of 1997 on the Processing and Protection of Personal Data relating to Health and Related Personal Data ("Eüak.") taking into account the resolutions and guidelines issued by the of the National Authority for Data Protection and Freedom of Information ("NAIH").

The purpose of the Policy is to set out the rules governing the processing of personal data (and in particular the processing of personal data including, without limitation, personal data concerning health which fall within a special category of personal data) and to ensure compliance with the constitutional principles of data protection, the protection of personal data and the right to information and data security.

The personal scope of this Policy covers all persons employed or otherwise engaged by the Company and to any person who has access to personal data processed by the Company the personal data processed by the Company on the basis of a contractual relationship.

For data security and for the protection of personal data processed and stored in the Company's electronic systems the provisions of the Company's IT Policy and the provisions of this Policy apply and shall be interpreted in accordance with the provisions of the other Company's policies. In case of any conflict between the provisions of this Policy and any other Policy of the Company, the provisions of this Policy shall prevail over the provisions of any other policies which have entered into force before the entry into force of this Policy. The Company establishes a separate policy on processing of personal data of employees.

1. Data Controller’s Contact Details

Name: Neunos Medical Device Development and Services Limited Liability Company
Abbreviated name: Neunos Zrt.
Registered office: H-6725 Szeged, Szécsi str. 14.
Place of business: 6720 Szeged, Dóm square 10 - 12.
Representative: Tamás Gyurkovics, Chief Executive Officer
Website: www.neunos.com
Electronic contact: info@neunos.com
Name and contact details of the Data Protection Officer: Dr. Viktória Papp, dpo@neunos.com
This Policy is available at: www.neunos.com

2. Definitions and Abbreviation

(1) The definitions in this Policy are the same as in Article 4 of the GDPR [Definitions] and the interpretative definition set out in Article 3 of the Infotv. [Explanatory Provisions].

(2) The following abbreviations shall be applied in this Policy:

- **GDPR** - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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);
- **Infotv.** - Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Infotv.");
- **Eüak.** – Act XLVII of 1997 on the Processing and Protection of Personal Data relating to Health and Related Personal Data (“Eüak.”);
- **NAIH** - National Authority for Data Protection and Freedom of Information;
- **OMIII** - National Institute of Mental Health, Neurology and Neurosurgery;
- **EESZT** - Electronic Health Service Space.

3. Basic Provisions and Principles Governing Data Management and Data Management Register

3.1. Basic Provisions and Principles Governing Data Management

(1) During processing personal data, the Company shall comply with the provisions of Chapter 2 of the GDPR and Chapter 2 of the Infotv. during the course of its activities, and the Company shall carry out the following activities in accordance with the applicable legislation processing of personal data. In any case, prior to collecting and processing personal data, the Company shall inform the data subject about the circumstances of the processing.

(2) The Company will only collect personal data for clearly defined, legitimate purposes, the exercise of a right and rights and obligations and in compliance with the purpose limitation principle, in accordance with this Policy and in the information, notices annexed to the Policy. Personal data will be processed by the Company only to the extent and for the time necessary for the purposes for which they are collected, in accordance with the Article 6-10 of the GDPR.

(3) While respecting the principles of purpose limitation and data minimisation, the Company stipulates that if the purpose of the processing ceases, the data will be deleted. The Company shall inform the data subject about the deletion data, involving the Company's Data Protection Officer, if necessary.

(4) By making this Policy available on the website, the Company is in compliance with the legal requirement for transparency of data processing operations and ensures compliance with the law. Processing activities of the data controller must be clear, easy and transparent, along the purposes of the processing, in accordance with Articles 13-14 of the GDPR. The privacy notice applicable only to employees of the Company make it available in a closed IT system in the form of internal policy.

3.2. Data Management Register

(1) The Company, as data controller, through the Data Protection Officer, shall establish a data management register in a closed and confidential system regarding its activities in accordance with Art. 30 of GDPR and Article 25/E of Infotv.
(2) The Company's Data Protection Officer shall keep the data management register up-to-date.
(3) The data management register shall be made available upon written request to the Company's Data Protection Officer.

4. The Company's Built-in and Default Data Protection System

4.1. Data Protection Impact Assessment

(1) If the Company intends to introduce a new data processing activity, the Data Protection Officer assess whether the conduct of a data protection impact assessment is in accordance with the requirements of Article 35 of the GDPR. If the Company intends to introduce a new processing activity and the nature of the new processing activity, scope, circumstances and objectives of the new data processing activity, or the technological solutions used, are likely to present a high risk of to the data subject, or the proposed processing is likely to give rise to a high risk for the data subject, or the proposed processing is in the list of Article 35(4) of the GDPR (https://naih.hu/hatasvizsgalati-lista), then a data protection impact assessment shall be conducted. The criteria for the impact assessment are set out in the Annex to this Policy (Annex 1).
(2) The results of the mandatory impact assessment carried out in respect of the health data processed by the Company can be obtained from the Company's Data Protection Officer by sending a written request to the Data Protection Officer's e-mail address.
(3) The impact assessment shall include at least a systematic description of the envisaged data processing operation and the purposes of the processing, the necessity and proportionality of the processing operations (balancing test), the risks to the rights and freedoms of the data subject and the measures to address the risks (safeguards, security measures).
(4) If the impact assessment carried out concludes that the processing is likely to result in a high risk, the Company shall, prior to processing personal data, consult the NAIH.

4.2. Ensuring Protection of Personal Data

(1) The Company applies up-to-date, closed, comprehensive and continuous organizational and technical protection measures which guarantee the confidentiality, integrity and availability of the personal data the Company manages and the Company ensures that the technological development is proportional to the risks appearing for the data subjects.
(2) Among the organisational protection measures:
2.1 The Company's Chief Executive Officer shall ensure that the provisions of this Policy are acknowledged by all employees. For complying with the provisions contained in this Policy every employee is responsible during the course of their duties. The Company shall ensure that the employees who process personal data and employees who have access to such data enter into a confidentiality agreement with the Company.

2.2 Persons employed by the Company during the performance of their duties are obliged to ensure that unauthorized persons should not be able to look into documents that include the personal data of data subjects, and persons employed by the Company should also ensure that documents contain the personal data of data subjects should not be accessible, changeable, destroyable or readable to unauthorized persons.

2.3 The Company keeps paper documents containing personal data securely locked, in a fire-protected place. For documents that are under permanent active management shall be accessible only to authorized persons. In case of processing of paper-based personal data has been achieved, the Company shall arrange for destroying the paper documents.

2.4 The Company appointed a Data Protection Officer in order to ensure and fulfill the highest level of data protection and to adhere to the legal requirements for handling personal data of data subject. The name and contact details of the Data Protection Officer are set out in this Policy and she/he has been introduced to NAIH.

2.4.1 The status of the Data Protection Officer:

2.4.1.1. she/he reports directly to the Chief Executive Officer;

2.4.1.2. she/he performs her/his duties independently and autonomously, she/he cannot be dismissed or sanctioned for the performance of her/his duties;

2.4.1.3. she/he informs the data subjects on the processing of their personal data and of their rights in relation to the processing;

2.4.1.4. in the performance of its tasks, she/he is bound by confidentiality obligations and the confidentiality of personal data.

2.4.2 The Data Protection Officer's tasks in relation to data protection include in particular:

2.4.2.1. she/he assists in ensuring the rights of data subjects;

2.4.2.2. she/he provides the Company with information and assistance in relation to data protection;

2.4.2.3. she/he participates in the conduct of the data protection impact assessment;

2.4.2.4. at the Company's request, she/he raises awareness of data protection issues for the Company by providing data protection training to the Company;

2.4.2.5. she/he keeps up-to-date the data protection registers pursuant to Article 30 of GDPR;

2.4.2.6. in the event of a data protection incident, she/he participates in the investigation of a data protection incident and, if necessary, inform the NAIH without delay (but no later than 72 hours);

2.4.2.7. she/he controls within the Company that the data protection procedures comply with the provisions of the present Policy and the provisions on applicable data protection legislation;

2.4.2.8. she/he liaises with the NAIH and cooperates with the authority in any investigation or proceeding initiated by the Authority;

2.4.2.9. she/he monitors changes in data protection legislation, and, where justified, initiates amendments to this Policy.

2.5 If the Company uses a data processor for the performance of its activities, then – in accordance with Article 28 of the GDPR – the liability of the data processor shall be laid down in a contract between the

Company and the data processor. The Company will only use data processor who provides adequate guarantees to ensure compliance with the requirements of the GDPR and to protect the rights of data subjects, and the protection of data subjects' rights.

(3) Among the technical protection measures:

3.1 For the Company's electronic systems - and thus for the personal data stored therein – only employees have access, for whom it is essential to get access to perform their duties.

3.2 The electronic devices used by the Company must have at least a unique user name and password protection.

3.3 In case of implementation of the purpose of data management with regard to the personal data stored in the electronic system and in case of expiration of the deadline of data management, the file containing the personal data shall be irretrievably deleted.

3.4 The Company is constantly monitoring the virus protection of its electronic systems and prevents unauthorized persons from accessing personal data processed on its network by using the available IT tools.

3.5 The Company laid down the rules for the electronic systems used (including both hardware devices and software), for the authorization levels for access and electronic systems in the IT Policy, so the IT Policy regarding the use of IT tools is applicable in addition to this Policy.

3.6 Specific provisions on the protection of health data:

3.6.1 Based on clinical research conducted in collaboration with OMIII, the Company handles health data of persons participating in clinical research, during which the Company receive data from OMIII from its internal IT system on a closed, IT-protected encrypted network by uploading to a storage (hereinafter: “storage”) in an anonymized, coded form. The OMII is responsible for uploading health data to EESZT. Patients included in the study are informed of the start of data processing, the OMIII shall obtain the consent of the data subject, together with the data management information sheet.

3.6.2 Within the Company, only those persons who carry out the data movement can access the health data available in storage. Health data will be deleted from the closed storage immediately after data movement. Storage access is possible via VPN, authorized persons who have reading rights can access the data available on the storage site and only a group of authorized persons has editing rights.

3.6.3 Files containing health data are encrypted, hiding the identity of the data subject and the Company handles them as an encrypted file, anonymised in a private, locked, electronic systems.

3.6.4 The electronic documents containing health information will be stored separately from other documents in a password-protected folder system, to which only authorized persons can have access who are necessarily involved in the evaluation of health data for research purposes.

3.6.5 The Company shall immediately destroy the health data immediately after the health data have been processed for the purpose for which they were collected.

4.3. Procedure for Handling Data Protection Incidents

(1) Taking into account the principles set out in the GDPR and prior to the start of data processing, the Company shall in all cases during its data processing activities establish the technical and organisational measures that are appropriate to the nature, scope, circumstances and purposes of the processing, the varying degrees of risk to the rights and freedoms of the persons concerned an appropriate level of data security proportionate to the risks.
(2) If a person employed by the Company suspects that a data breach has occurred, she/he shall immediately inform the Company's Chief Executive Officer about all the circumstances of the incident. If the available information clearly establishes that a personal data breach has occurred, the Company will take all available technical and organizational measures to ensure to reduce the impact of the incident on the data subjects and shall immediately notify the Data Protection Officer by completing the notification form (NEU-TMP-085).
(3) In carrying out the tasks under Section 4.2 of this Policy, care should be taken to ensure that the data breach shall be notified to the NAIH within 72 hours of its occurrence, unless it is unlikely to pose a risk to the rights of data subjects.
(4) The Data Protection Officer will examine the information contained in the notification as described above and assess the data breach and determine the potential impact of the data breach and, if necessary, involve the person responsible for information security, the Chief Executive Officer and the person responsible for the data breach. If data breach has occurred when the Company used a data processor, the representative of the data processor shall be involved in the investigation.
(5) As part of the investigation, the Data Protection Officer measures the data protection incident and informs the parties -including the Chief Executive Officer of the Company- about the results of the investigation. If, as a result of the investigation, it is established that the data protection incident is likely to pose a risk to the rights and freedoms of the data subjects, the Data Protection Officer reports the data protection incident to NAIH according to Article 25/K. of the Infotv. and informs the person concerned.
(6) The Company, through the Data Protection Officer, will keep a separate record of any data protection incidents that occur in accordance with Article 33(5) of the GDPR.

5. Certain Data Processing Activities of the Company

5.1. Processing of Personal Data of Applicants Applying for Positions to be Filled

(1) The Company publishes vacancies on its website and on job advertising portals. The Company does not use anonymous job advertisements and does not use recruitment agencies. Applicants may apply directly for positions advertised by the Company or by e-mail to info@neunos.com.
(2) The Company informs all candidates whether the application for a given position was successful or not.
(3) Circumstances of processing of personal data of applicants for vacant positions:
Purpose of processing: to fill vacant positions and, if successful, to establish an employment relationship
Scope of data processed: name, e-mail address, telephone number, other personal data provided by the applicants concerned, or other data available on the CV

Source of data processed: directly from the data subject
Legal basis for processing: data subject's consent pursuant to Article 6(1)(a) of GDPR
Data retention period: until the vacant position is filled
Method of data storage: electronically
Data subject's rights: according to Chapter 6 of this Policy

5.2. Processing of Data Related to Contracts and Invoicing

(1) The Company is also aware of the data protection regulations set out in the GDPR and Infotv with regard to the contracts it has entered into. As a result of which in relation to Company's contracts, which are concluded with natural persons or with legal persons or with companies without legal personality where other contributors during the performance of the contract does not participate in data management, the Company carry out its activities as follows:
Purpose of processing: performance of the contract
Scope of data processed: name of the legal representative, other personal information specified in the contract
Source of data processed: directly from the data subject
Legal basis for processing: Article 6(1)(b) GDPR [performance of contract]
Data retention period: until performance of the contract or, after termination of the contract, the Company shall retain the personal data of the legal representative of the Company for the purpose of asserting and protecting legal claims arising from the contract in accordance with the general rules on period of limitation under the Hungarian Civil Code and the Act C of 2000 on Accounting (8 years)
Method of data storage: electronic and paper (if the contract concluded is paper-based)
Data subject's rights: according to Chapter 6 of this Policy
(2) In respect of contracts entered into by the Company with legal persons or legal entities where the performance of the contract involves other natural persons on the side of the contracting party, the Company shall process the personal data of the contributors as follows:
Purpose of processing: performance of the contract and the necessary contacts for this purpose
Scope of data processed: name of the contact person, other personal data provided in the contract
Source of data processed: contract
Legal basis for processing: Article 6(1)(f) GDPR [legitimate interest of the Company)
Data retention period: until performance of the contract
Method of data storage: electronically and on paper (if the contract concluded is paper-based)
Data subject's rights: in accordance with Chapter 6 of this Policy
(3) In respect of contracts for which the Company receives invoices and makes payments, the Company shall, in respect of the personal data contained in the supporting documents relating to the invoice, disclose the following data processing activities:
Purpose of the processing: establishing mandatory data content of the invoice received by the Company regarding accounting tasks
Scope of data processed: data contained in the invoice and related supporting documents
Legal basis for processing: legal obligation pursuant to Article 6(1)(c) of the GDPR (Art. 159§ (1) of the Act CXXVII of 2007 and Art. 169§ (1) of the Act C of 200)

Data retention period until the deadline laid down in the Art. 169§ (1) of the Act C of 2000 – 8 years
Method of data storage: electronic and paper-based (if the invoice is also paper-based available on paper)
Data subject's rights: in accordance with Chapter 6 of this Policy

5.3. Processing of Data Related to Company's Contracts

The Company processes the personal data provided by persons contacting the Company in the following ways:
Purpose of processing: maintaining contact with persons contacting the Company and communication
Scope of the data processed: name, e-mail address, telephone number of the data subject, other personal data provided by the data subject
Legal basis for processing: data subject's consent pursuant to Article 6(1)(a) of the GDPR
Data retention period: until withdrawal of consent. The consequence of the withdrawal of consent is that the Company will not be able to contact the data subject after the withdrawal. The withdrawal of the consent shall not affect the lawfulness of the consent.
Method of data storage: electronically
Data subject's rights: according to Chapter 6 of this Policy

5.4. Processing of Health Data

(1) In addition to the provisions laid down in the GDPR and Infotv., the Company conducts clinical research and respects the data subject's personal and health data contained in the Eüak. The Company acknowledges that the respective person's health personal data for the purpose of joint scientific research with OMIII (as a research site) managed in accordance with Section 4, paragraph (1) point d) of Eüak.
(2) Processing of data for the primary purpose of clinical trials in clinical research, i.e., the study of the data subjects, is carried out by OMIII in its entirety, so that the data management information, which forms part of the trial prospectus and the consent form is presented and accepted by the OMIII to the subject (data subject) or legal representative. The Company shall handle, for secondary purposes related to clinical trials, i.e., for the purpose of scientific research, the health and medical data of the data subject's personal data. Regarding data management activities for secondary purposes the Company prepares and accepts a detailed data management information sheet with the affected parties or with their legal representatives.
(3) With regard to the processing of health data, the Company respects the provisions of Article 9 of the GDPR, on the processing of special categories of personal data, under which the Company processes health data as follows:
Purpose of processing: for the Neunos SeizureSTOP™ NeuroClinical system of Neunos Zrt., as concerning a medical device, the Eüak. lays down in Art. 4 (1) point d) the evaluation of the results of clinical research and publication of the results
Scope of medical data processed: magnetic resonance imaging (MRI) scan, electroencephalogram (EEG) scan, video recordings during the examination, medication data
Scope of personal data relating to the health data processed: name, place of birth, date, social security number, subject's mother's name, address
Source of the data processed: directly from the data subject or, with consent, from OMIII

Legal basis for processing: *explicit consent of the data subject* as set out in Art. 4 (4) of Eüak, Art. 6 (1) a) of GDPR and Art. 9 (1) of GDPR; the *legitimate interest of the Company* as set out in Art. 6 (1) f) of GDPR; and when the processing of health data is necessary for reasons of public interest such as high quality and safety of medical devices and to ensure that the processing is necessary for *scientific research purposes* according to Art. 9 (i) of GDPR. In addition to this, Art. 4 (2) point d) of Eüak. which states that health and personal data may be processed for the purposes of scientific research. In view of the above legal bases and the fact that the Company's purpose with the processing of personal and health data is evaluating the results of clinical research, publishing the results in a scientific publication, and using the research result in an anonymized way, the processing of data (both voluntarily and explicit consent) is carried out by the Company in accordance with the European Data Protection Board Opinion No 3/2019 and the Medical Research Council - Clinical Pharmacology Ethics Committee's Recommendation on clinical trials.

Data retention period: 5 years from the end of the research or until withdrawal of consent. The consequence of withdrawal of consent is that the subject will no longer participate in clinical research. The lawfulness of the data processing prior to withdrawal is not affected by the withdrawal of consent. Pursuant to Article 17(3)(d) of the GDPR, the withdrawal of consent may be refused if it is likely to undermine or seriously compromise the scientific research.

Data storage: electronically

Transfer of data: the legal basis for the transfer of data is the contract between OMII and the Company based on Art. 6 (1) b) of GDPR. In addition, a further legal basis for the transfer of data is Art. 6 (1) a) of the GDPR and the data subject's consent pursuant to art. 9 (2) a) of GDPR, and achieving the higher objectives in accordance with Art.9 (2) i) and j) of GDPR (i.e. ensuring high quality and safety of medical devices, scientific research objectives)

Uploading data to the EESZT: in accordance with 39/2016 (XII.21.) Regulation of Ministry of Human Capacities and with Eüak., OMIII is required by to upload the health data relating to clinical research and related personal data of its patients to the EESZT in cooperation with the State Health Care Centre. (The EESZT data management information is available here: https://e-egeszsegugy.gov.hu/documents/26398/557047/EESZT_Lakossagi_adatkezelesi_tajekoztato_2021_v6.pdf/8678cf08-dbec-407d-03a9-f8e34e22fa43)

Data subject's rights: as set out in Chapter 6 of this Policy

5.5. Website-related Data Management

The Company has its own website: www.neunos.com

Anyone can access the website operated by the Company without revealing their identity or providing their personal data, obtain freely and without restrictions information on the website and the pages linked to it. However, non-personal information is collected unlimitedly and automatically by website about visitors. However, no personal data can be obtained from these data, so the GDPR or Infotv. does not implement data management under its scope.

6. Rights of the Data Subject

6.1. Right of Access by the Data Subject

(1) The data subject shall have the right to obtain from the Company information about the processing of her/his personal data by contacting the Company at the contact details indicated.
(2) The Company will respond to a request in relation to processing of personal data of the data subject within 25 days – in case of exercising the right to object this is 15 days - in writing and in a comprehensible form.
(3) The information shall include the information specified in Article 15(1) of the GDPR, provided that the information cannot be refused by law. The Company shall take appropriate measures to ensure to provide the data subject with the information in relation to processing of personal data in accordance with Articles 13 and 14 of the GDPR and Articles 15 to 22 and 34 of the GDPR, in a transparent, intelligible and easily accessible way and in a clear and plain language. The information shall be provided in writing or by other means, including, where appropriate, by electronic means. Oral information may be provided at the request of the data subject, if the identity of the data subject is demonstrated.
(4) As a general rule, the information is provided free of charge and the Company will only charge a fee incurred pursuant to Article 12 (5) a) of the GDPR.
(5) The Company shall refuse a request only on the grounds set out in Article 12(5)(b) of the GDPR and shall do it only with a statement of reasons, with appropriate information in writing.

6.2. Right to Erasure ('right to be forgotten")

(1) The Company shall correct information that does not correspond to reality - as long as it is the necessary data and the proof thereof in public documents are available – and in the event of the existence of the reasons specified in Article 17 of the GDPR. The Company arranges for erasure of processed personal data.
(2) The data subject shall have the right to obtain from the Company the erasure of personal data concerning her/him without undue delay and the Company shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent and where is no other legal ground for the processing;
- the data subject objects to the processing and where there is no other legal ground for the processing;
- the personal data have been unlawfully processed by the Company.

6.3. Right to Object

(1) The data subject shall have the right to object the processing of her/his personal data at any time by means of notification, especially if personal data is handled or transmitted exclusively for the Company's law enforcement, except in the case of mandatory data processing required by the law.

(2) For the duration of the assessment of the objection to the processing of the data subject's personal data, the Company suspends the data management – but no more than 5 days – and examines the merits of the objection and makes a decision, about which the Company informs the applicant in accordance with Article 19 of the GDPR.
(3) If the objection is justified, the Company shall act in accordance with Article 21 of the GDPR.
(4) If the Company establishes that the data subject's objection is well-founded, then the Company terminates and locks the data processing - including further data collection and data transmission –and notifies all to whom the personal data – that is subject of the objection – was previously transferred.
(5) If the data subject does not agree with the Company's decision or if the Company fails to respond within the time limit, the data subject may -within 30 days from the announcement of the decision or the last day of the deadline- take the matter to court.
(6) The Company may not delete the data of the data subject if the processing is required by law.

6.4. Right to Restriction of Processing

The data subject shall have the right to obtain from the Company restriction of processing, if:

- the accuracy of personal data is contested by the data subject (for a period enabling the Company to verify the accuracy of the personal data)
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) of GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject. (in this case, the limitation for that period applies until it is determined whether the Company's legitimate reasons takes precedence against the legitimate reasons concerned).

6.5. The Right to Data Portability

The Company's processing activities as set out in this Policy do not give rise to any processing that would require the provisions of data portability.

6.6. Automated Individual Decision-making, Including Profiling

Automated individual decision-making or profiling takes no place during the course of the Company's data management activities.

6.7. Right to Compensation and Liability due to Unlawful Processing

(1) By unlawfully processing the data of the data subject or by breaching the requirements of data security, the Company may compensate any damage caused to another person. In addition, the Company compensates the damages for personal injury caused by the Company or by a data processor used by the Company.
(2) The Company is exempted from liability for the damage caused and the from the obligation to pay damages, if it proves that the damage to the data subject's personal data was caused by an unforeseeable

event outside the scope of the processing activities. The Company also does not compensate for damage, if it was caused intentionally or through gross negligence on the part of the injured party.

6.8. Access to Judicial Remedy

(1) The data subject has the right to lodge a complaint with the Company's Data Protection Officer (Dr. Viktória Papp; dpo@neunos.com) directly or, at his/her option, with to the National Data Protection and Privacy Authority (1055 Budapest, Falk Miksa utca 9-11; postal address: 1363 Budapest, Pf. 9.) or with the court where the data subject has her/his habitual residence.
(2) In the context of processing activities of the data processor, the data subject may take the Company or the data processor to court, if the data subject is of the opinion, that the Company or data processor acting on behalf of the Company infringe the data subject's rights laid down in the applicable legislation and in the binding acts of the European Union.
(3) The court shall handle such disputes with priority over others.

_____

Tamás Gyurkovics
CEO
Neunos Zrt.

7. Attachments

Annex 1 - Criteria for conducting a data protection impact assessment

8. Documentation

Documentation created according to this policy shall be prepared, reviewed and approved in accordance with Control of Documents quality management procedure.

8.1. List of Deliverables

- Data Breach Notification/Adatvédelmi Incidens bejelentő lap (NEU-TMP-085)

9. References

- **GDPR** - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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);
- **Infotv.** - Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Infotv.");
- **Eüak.** – Act XLVII of 1997 on the Processing and Protection of Personal Data relating to Health and Related Personal Data ("Eüak.")
- NEU-QM-008 Documentation Management

10. Annex 1

Criteria for conducting a data protection impact assessment

The Company intends to implement the following data management procedure in connection with the performance of its activities, whereby the Company acts as data controller:

1) Description of the data management process to be implemented:
2) A systematic description of the data processing operations:
3) Identification of the Company and other participants in the data management process (description of the status of the participants and their activities related to data management):
4) Expected date of implementation of the processing:

Article 6(1)(a) to (f) of the GDPR shall apply when examining the legal basis for processing.
If the legal basis is Article 6(1)(f) of the GDPR: the processing will be lawful if and insofar as the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.
In order to assess the lawfulness of the processing, a balancing of interests' test should be carried out, whereby the necessity of the purpose of the processing and the proportionality of the restriction of the rights and freedoms of the data subjects should be assessed and duly justified.
The Company will carry out the following impact assessment as indicated by Article 35 of the GDPR:

1) **Legal basis for processing**
2) **Purpose of the processing/description of the legitimate interest of the controller**

A description of the purposes and reasons for the processing, in particular the necessity and indispensability of the processing:

1) **Precise definition of the scope of the data processed.** Determination of the specific purposes for which the data are processed.
2) **Data subjects**
3) **Other circumstances of processing**
4) **Circumstances of the transfer** (recipient, purpose, legal basis)
5) **Expected impacts, risks**
   What are the potential risks of the processing in terms of possible prejudice to the rights of data subjects? Data security risks assessment. The possible occurrence of possible data loss, unauthorised access or other data breaches, and the likelihood of an incident occurring.
6) **What are the interests of data subjects in relation to the processing** (are the restrictions on data subjects' rights proportionate to the aim to be achieved? Are the rights of data subjects limited only to the extent necessary to achieve the purpose?)
7) **Finding alternatives.** Is there another way to achieve the objective that is less restrictive of the rights of data subjects? If so, is it as effective in achieving the objective?
8) **Measures taken to address the risks, safeguards, cooperation of the parties**

9) **Description of the measures taken** (to what extent each measure reduces the risks of data processing. Description of data security measures (physical, logical, administrative measures taken).
10) **Ensuring cooperation with data subjects** (possibilities for redress, possibility to provide information upon request, existence of a data protection policy, appointment of a data protection officer, etc.).
11) **Stating the outcome of the impact assessment** (description of the extent and nature of the risk, whether further action is necessary, whether prior consultation is necessary, description of the extent and nature of the risk, conclusion (why the processing is lawful, why there is a higher interest in achieving the objective, and what is the proportionality of the restriction of the rights of the data subjects).
12) **Description of data subjects' rights, right to object, right of access**

Belső Adatvédelmi és Adatbiztonsági Szabályzat

A Neunos Zrt. (továbbiakban: Társaság) az Információs önrendelkezési jogról és az információszabadságról szóló 2011. évi XII. törvény (továbbiakban: Infotv.), az Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679. számú Rendelete (továbbiakban: GDPR), továbbá az egészségügyi adatok tekintetében az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (továbbiakban: Eüak.) rendelkezései alapján az alábbi Belső Adatvédelmi és Adatbiztonsági Szabályzatot (továbbiakban: Szabályzat) alkotja meg, figyelembe véve a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH) által kiadott állásfoglalásokat és iránymutatásokat is egyaránt.

A Szabályzat célja, hogy meghatározza a Társaságnál folytatott személyes adatok (és azon belül különös figyelemmel a személyes adatok különleges kategóriájába tartozó egészségügyi személyes adatok) kezelésének jogszerű rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

A Szabályzat személyi hatálya kiterjed a Társasággal munkaviszonyban vagy egyéb foglalkoztatásra irányuló jogviszonyban álló személyre továbbá minden olyan személyre, akik a Társaság által kezelt személyes adatokhoz hozzáféréssel rendelkeznek a Társasággal fennálló szerződéses jogviszony alapján.

A Társaság elektronikus rendszereiben kezelt és tárolt személyes adatok védelmére irányuló adatbiztonsági követelményeket a Társaság IT Szabályzatában lévő rendelkezésekkel, egyebekben jelen Szabályzat rendelkezéseit a Társaság többi Szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok kezelésével kapcsolatosan ellentmondás áll fenn jelen rendelkezések és a bármely más, jelen Szabályzat hatálybalépése előtt hatályba lépett Szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadóak. A Társaság a munkavállalók személyes adatainak kezelésére vonatkozóan különálló szabályzatban rendelkezik

11. Adatkezelő Elérhetőségei

Név: Neunos Orvosi Műszerfejlesztő és Szolgáltató Zártkörűen Működő Részvénytársaság
Rövidített név: Neunos Zrt.
Székhely: 6725 Szeged, Szécsi u. 14.
Telephely: 6720 Szeged, Dóm tér 10 – 12.
Képviselő: Gyurkovics Tamás vezérigazgató
Weboldal: www.neunos.com
Elektronikus elérhetőség: info@neunos.com
Adatvédelmi tisztviselő neve, elérhetősége: Dr. Papp Viktória, dpo@neunos.com
Jelen Szabályzat elérhető: www.neunos.com

12. Fogalmak, Rövidítések

(1) A jelen Szabályzat fogalmi rendszere megegyezik a GDPR 4. cikkében [fogalommeghatározások] illetve az Infotv. 3. pontjában [Értelmező rendelkezések] meghatározott értelmező fogalom magyarázatokkal.
(2) A jelen Szabályzatban használt rövidítések:

a. **GDPR** – az Európai Parlament és Tanács (EU) 2016/679 számú rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (Általános Adatvédelmi Rendelet);
b. **Infotv.** – az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;
c. **Eüak.** – az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény;
d. **NAIH** – Nemzeti Adatvédelmi és Információbiztonsági Hatóság;
e. **OMIII** – Országos Mentális, Ideggyógyászati és Idegsebészeti Intézet;
f. **EESZT** – Elektronikus Egészségügyi Szolgáltatási Tér

13. Az Adatkezelésre Vonatkozó Alapvető Rendelkezések, Alapelvek, az Adatkezelési Nyilvántartás

13.1. Adatkezelésre Vonatkozó Alapvető Rendelkezések, Alapelvek

(1) A Társaság a személyes adatok kezelése során a GDPR II. fejezetében illetve az Infotv. II. fejezetében foglaltakra tekintettel rögzíti, hogy tevékenysége során a hatályos jogszabályok alapján végez adatkezelést. A Társaság minden esetben a személyes adatok felvételét, kezelését megelőzően tájékoztatja az érintetteket az adatkezelés körülményeiről.
(2) A Társaság személyes adatot kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében, a célhoz kötöttség elvét tiszteletben tartva kezel a jelen szabályzatban illetve a szabályzat mellékletét képező adatkezelési tájékoztatókban foglaltak szerint. A személyes adatot a Társaság csak a cél megvalósulásához szükséges mértékben és ideig kezeli a GDPR 6. – 10. cikkében meghatározott jogalap birtokában.
(3) A célhoz kötöttség és az adattakarékosság elvét tiszteletben tartva a Társaság rögzíti, hogy amennyiben az adatkezelés célja megszűnt, az adatok törlésre kerülnek. A törlésről a Társaságnak az adatot ténylegesen kezelő munkavállalója gondoskodik, szükség esetén bevonva a Társaság adatvédelmi tisztviselőjét.
(4) A Társaság az adatkezelési műveletek átláthatóságára vonatokozó jogszabályi követelménynek való megfelelés érdekében adatkezelési tevékenységéről az adatkezelés érintettjei számára világos, könnyen értelmezhető és átlátható módon, az adatkezelés céljai mentén a GDPR 13-14. cikke szerinti tartalommal jelen szabályzatban foglalt tájékoztatást nyújt azzal, hogy a jelen szabályzatot honlapján közzéteszi, míg a kizárólag a Társaság által foglalkoztatottakra vonatkozó adatkezelési tájékoztatót belső szabályzat formájában zárt informatikai rendszerben teszi elérhetővé.

13.2. Az Adatkezelési Nyilvántartás

(1) A Társaság az adatvédelmi tisztviselő útján adatkezelési tevékenységeiről a GDPR 30. cikkének illetve az Infotv. 25/E. §-ában foglaltaknak mindenben megfelelő adattartalommal, zárt informatikai rendszerben elektronikus adatkezelői nyilvántartást vezet.
(2) A nyilvántartás naprakészen tartását a Társaság adatvédelmi tisztviselője végzi.
(3) Az adatkezelési nyilvántartás a Társaság adatvédelmi tisztviselőjéhez intézett írásbeli kérelemre kikérhető.

14. A Társaság Beépített- és Alapértelmezett Adatvédelmi Rendszere

14.1. Adatvédelmi Hatásvizsgálat

(1) Amennyiben a Társaság új adatkezelési tevékenység bevezetését tervezi, úgy adatvédelmi tisztviselő bevonásával megvizsgálja, hogy az adatvédelmi hatásvizsgálat lefolytatásának a GDPR 35. cikkében foglalt feltételei fennállnak-e. Amennyiben a Társaságnál bevezetendő új adatkezelési tevékenység annak jellege, hatóköre, körülményei és céljai, vagy az alkalmazott technológiai megoldások kapcsán az magas kockázattal jár az érintettre nézve, vagy a tervezett adatkezelés a NAIH-nak a GDPR 35. cikk (4) bekezdése szerint összeállított jegyzékében szerepel (https://naih.hu/hatasvizsgalati-lista), úgy adatvédelmi hatásvizsgálatot folytat le. A hatásvizsgálat szempontrendszerét a jelen szabályzat melléklete tartalmazza.
(2) A Társaság által kezelt egészségügyi adatok tekintetében elvégzett kötelező hatásvizsgálat eredménye a Társaság adatvédelmi tisztviselőjétől kikérhető az adatvédelmi tisztviselő e-mail címére küldött írásbeli kérelem formájában.
(3) A hatásvizsgálat kiterjed legalább a tervezett adatkezelési művelet módszeres leírására és az adatkezelés céljainak ismertetésére, az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára (érdekmérlegelési teszt), az érintett jogait és szabadságait érintő kockázatok vizsgálatára és a kockázatok kezelését célzó intézkedések bemutatására (garanciák, biztonsági intézkedések).
(4) Amennyiben az elvégzett hatásvizsgálat azt állapítja meg, hogy az adatkezelés valószínűsíthetően magas kockázattal jár, akkor a Társaság a személyes adatok kezelését megelőzően konzultációt kezdeményez a NAIH-nál.

14.2. A Személyes Adatok Védelmének Biztosítása

(1) A Társaság a kezelésében lévő személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását biztosítandó, az érintettekre nézve megjelenő kockázatokkal arányos, a technológiai fejlődés szempontjából naprakész, zárt, teljes körű és folytonos szervezési és technikai védelmi intézkedéseket alkalmaz. A Társaság által kezelt személyes adatok védelméért, az adatkezelés jogszerűségéért a Társaság vezető tisztségviselője felel.
(2) A szervezési védelmi intézkedések körében:
2.1 A Társaság vezető tisztségviselője biztosítja, hogy a szabályzatban foglaltakat minden foglalkoztatott megismerje és betartsa. A jelen szabályzatban foglalt rendelkezések betartásáért a feladatkörében

minden munkavállaló felelős. A Társaság gondoskodik arról, hogy a személyes adatokat kezelő és azokhoz hozzáféréssel rendelkező foglalkoztatottak Titoktartási megállapodást kössenek a Társasággal;

2.2 A Társaság által foglalkoztatott személyek kötelesek arra, hogy feladataik ellátása során jogosulatlan személyek ne tekinthessenek be olyan dokumentumokba, amelyek az érintettek személyes adatait is tartalmazhatják, továbbá gondoskodnak arról, hogy az érintettek személyes adatait is tartalmazó dokumentumok jogosulatlan személyek számára ne legyenek hozzáférhetők, megismerhetők, megváltoztathatók, megsemmisíthetők;

2.3 A Társaság a papír alapon kezelt, személyes adatokat is tartalmazó dokumentumokat jól zárható, tűzvédelmi berendezéssel ellátott helyen tárolja. A folyamatosan aktív kezelésben lévő iratokhoz kizárólag az arra jogosult személyek férhetnek hozzá. Amennyiben a papír alapon tárolt személyes adatok kezelésének célja megvalósult, úgy a Társaság intézkedik annak megsemmisítéséről.

2.4 A Társaság az érintettek személyes adatainak kezelésére vonatkozó jogszabályi előírások teljesítésének és az érintetti jogok minél magasabb szintű biztosításának érdekében adatvédelmi tisztviselőt nevezett ki. Az adatvédelmi tisztviselő neve és elérhetősége jelen szabályzatban került feltüntetésre, valamint a NAIH számára bejelentésre került.

2.4.1 Az adatvédelmi tisztviselő jogállása:

2.4.1.1.közvetlenül a vezető tisztségviselőnek tartozik felelősséggel;

2.4.1.2 feladatait függetlenül és önállóan látja el, feladatai ellátásával összefüggésben el nem bocsátható, szankcióval nem sújtható;

2.4.1.3 az érintetteket a személyes adataik kezeléséhez és az adatkezeléssel összefüggő jogaik gyakorlásához kapcsolódó valamennyi kérdésben segíti;

2.4.1.4 feladatai teljesítésével kapcsolatban titoktartási kötelezettség, illetve az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

2.4.2 Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai különösen:

2.4.2.1 segítséget nyújt az érintettek jogainak biztosításában;

2.4.2.2 a Társaság számára tájékoztatást és segítséget nyújt az adatvédelemmel kapcsolatos jogszabályi rendelkezésekkel, kötelezettségekkel kapcsolatosan,

2.4.2.3 közreműködik az adatvédelmi hatásvizsgálat lefolytatásával kapcsolatosan;

2.4.2.4 a Társaság felkérésére az adatvédelmi tudatosság erősítése érdekében a Társaság számára adatvédelmi oktatást tart;

2.4.2.5 naprakészen vezeti a GDPR 30. cikke szerinti adatvédelmi nyilvántartást;

2.4.2.6 adatvédelmi incidens bekövetkezése esetén részt vesz annak kivizsgálásában és szükség esetén haladéktalanul (de legkésőbb 72 órán belül) tájékoztatja a NAIH-t;

2.4.2.7 a Társaságon belül ellenőrizheti, hogy az adatvédelmi folyamatok megfelelnek-e a jelen szabályzatban illetve az adatvédelemmel kapcsolatos jogszabályi rendelkezésekben foglaltaknak

együttműködik és kapcsolatot tart a NAIH-val, valamint közreműködik a Hatósággal a Hatóság által kezdeményezett vizsgálat, eljárás során;

2.4.2.8 figyelemmel kíséri az adatvédelemmel kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását.

2.5 Amennyiben a Társaság tevékenységeinek ellátása érdekében adatfeldolgozót vesz igénybe, úgy a GDPR 28. cikke szerinti tartalommal az adatfeldolgozó felelőssége önálló adatfeldolgozói szerződésben vagy a Társaság és az adatfeldolgozó között létrejövő szerződés részeként kerül rögzítésre. A Társaság kizárólag olyan adatfeldolgozót vesz igénybe, amely megfelelő garanciákat nyújt a GDPR követelményeinek való megfelelés és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

(3) A technikai védelmi intézkedések körében:

3.1 A Társaság elektronikus rendszereihez – és így az abban tárolt személyes adatokhoz – kizárólag azon foglalkoztatottak rendelkeznek hozzáféréssel, akiknek a feladataik ellátásához ez elengedhetetlenül szükséges. 3.2 A Társaság által alkalmazott számítástechnikai eszközök legalább egyedi felhasználónévvel és jelszóval védettek.3.3 Amennyiben az elektronikus rendszerben tárolt személyes adat tekintetében az adatkezelés célja megvalósult vagy az adatkezelés határideje letelt, úgy az a személyes adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül.

3.4 A Társaság az elektronikus rendszereinek védelme tekintetében a vírusvédelemről folyamatosan gondoskodik, illetve a rendelkezésre álló informatikai eszközök alkalmazásával megakadályozza, hogy a hálózatán kezelt személyes adatokhoz illetéktelen személyek hozzáférjenek.

3.5 A Társaság az alkalmazott elektronikus rendszerekhez (beleértve a hardver eszközöket és szoftvereket is egyaránt) való hozzáférésre vonatkozó jogosultsági szinteket illetve az elektronikus rendszerek körét és használatukra vonatkozó részletszabályokat az IT Szabályzatában határozza meg, így az IT Szabályzat az informatikai eszközök használata tekintetében jelen szabályzat kiegészítéseként alkalmazandó.

3.6 Az egészségügyi adatok védelmére vonatkozó speciális rendelkezések:

3.6.1 A Társaság az OMIII-el közös együttműködésben folytatott klinikai kutatás alapján kezeli a klinikai kutatásban résztvevő személyek egészségügyi adatait, amely során az OMIII belső informatikai rendszeréből zárt, informatikai védelemmel ellátott titkosított hálózaton elérhető tárhelyre (továbbiakban: tárhely) való feltöltéssel, anonimizált, kódolt formában kerülnek a Társasághoz az egészségügyi adatok. Az egészségügyi adatok EESZT-be való feltöltésért az OMIII tartozik felelősséggel. A vizsgálatba bevont páciensekkel az adatkezelés megkezdését megelőzően az OMIII az adatkezelési tájékoztatóval egybekötött hozzájáruló nyilatkozatot beszerzi.

3.6.2 A Társaságon belül kizárólag csak azon személyek férhetnek hozzá a korlátozott hozzáférésű tárhelyen elérhető egészségügyi adatokhoz, akik az adatmozgatást végzik. A zárt tárhelyről az adatmozgatást követően haladéktalanul törlésre kerülnek az egészségügyi adatok. A tárhelyhez való hozzáférés VPN-en keresztül lehetséges, a tárhelyen elérhető adatokhoz a hozzáférésre jogosultaknak kizárólag olvasási jogosultságuk van és csak nagyon szűk azon hozzáférésre jogosultak köre, akik szerkesztési jogosultsággal is rendelkeznek.

3.6.3 Az egészségügyi adatokat tartalmazó fájlok titkosítva, az érintett személyazonosságát elrejtve kerülnek tárhelyre és a Társaság titkosított fájlként, anonimizált módon kezeli azokat saját zárt, elektronikai rendszereiben.

3.6.4 Az egészségügyi adatokat tartalmazó elektronikus dokumentumokat a Társaság az egyéb dokumentumoktól elkülönítve, jelszóval védett mapparendszerben kezeli, amelyhez a Társaságon belül

kizárólag csak azon személyek rendelkeznek hozzáféréssel, akik az egészségügyi adatok kutatási célú kiértékelésében szükségszerűen részt vesznek.

3.6.5 Az egészségügyi adatokat az adatkezelési cél elérését követően a Társaság haladéktalanul megsemmisíti.

14.3. Adatvédelmi Incidensek Kezelésével Kapcsolatos Eljárás

(1) A Társaság a GDPR-ban rögzített elveket figyelembe véve az adatkezeléssel járó folyamatainak megtervezése során az adatkezelés megkezdését megelőzően minden esetben kialakítja azokat a technikai és szervezési intézkedéseket, amelyek az adatkezelés jellegére, hatókörére, körülményeire és céljaira, valamint az érintett személyek jogaira és szabadságaira jelentett változó valószínűségű kockázatok figyelembevételével kockázatarányosan megfelelő szintű adatbiztonságot garantálnak.

(2) Amennyiben a Társaság által foglalkoztatott személy adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul tájékoztatja az eset összes körülményéről a Társaság vezető tisztségviselőjét. Amennyiben a rendelkezésre álló adatok alapján egyértelműen megállapítható az adatvédelmi incidens bekövetkezése, úgy a Társaság megtesz minden rendelkezésre álló technikai és szervezési intézkedést az incidens érintettekre gyakorolt hatásának csökkentése érdekében és haladéktalanul értesíti erről az adatvédelmi tisztviselőt a bejelentő lap kitöltésével (NEU-TMP-085).

(3) A 2. pontban foglalt feladatok elvégzése során figyelemmel kell lenni arra, hogy az adatvédelmi incidenst az annak bekövetkezésétől számított 72 órán belül be kell jelenteni a NAIH-nak, kivéve, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére.

(4) Az adatvédelmi tisztviselő megvizsgálja a fentiek szerinti értesítésben foglaltakat és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében szükség szerint bevonja a Társaságnál kijelölt, az informatikai biztonságért felelős személyt, a vezető tisztségviselőt és az adatvédelmi incidens bekövetkezésének gyanúját jelző személyt. Amennyiben az adatvédelmi incidens a Társaság által igénybe vett adatfeldolgozó tevékenységével kapcsolatban következett be, a kivizsgálásba az adatfeldolgozó képviselőjét is be kell vonni.

(5) Az adatvédelmi tisztviselő a vizsgálat keretében mérlegeli az adatvédelmi incidens következtében az érintettekre nézve megjelenő kockázatokat és a vizsgálat eredményéről tájékoztatja a Társaság ügyvezetőjét. Amennyiben a vizsgálat eredményeként megállapításra kerül, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintettek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő az adatvédelmi incidenst bejelenti a NAIH számára, illetve az Infotv. 25/K. §-ban foglalt esetben tájékoztatja az érintettet.

(6) A Társaság a bekövetkezett adatvédelmi incidensekről az adatvédelmi tisztviselő útján külön nyilvántartást vezet a GDPR 33. cikk (5) bekezdése szerint.

15. A Társaság Egyes Adatkezelési Tevékenységei

15.1. Betöltendő Pozíciókra Jelentkezők Személyes Adataival Kapcsolatos Adatkezelés

(1) A Társaság a megüresedett pozíciókat a honlapján közzéteszi illetve álláshirdető portálokon meghirdeti. A Társaság anonim álláshirdetést nem alkalmaz, munkaerő közvetítő cég közreműködését

nem veszi igénybe. A Társaságnál meghirdetett pozíciókra az érdeklődők közvetlenül jelentkezhetnek, vagy az info@neunos.com e-mail címen keresztül.
(2) A Társaság minden érdeklődőt tájékoztat arról, hogy az adott pozícióra történő jelentkezés sikeres volt-e vagy sem.
(3) A betöltendő pozíciókra jelentkezők személyes adataival kapcsolatos adatkezelés körülményei:
Adatkezelés célja: a megüresedett pozíciók betöltése és sikeres kiválasztás esetén munkaviszony létesítése
Kezelt adatok köre: név, e-mail cím, telefonszám, az érintett jelentkező által megadott egyéb személyes adatok, illetve az önéletrajzon elérhető egyéb adat
Kezelt adatok forrása: közvetlenül az érintettől
Adatkezelés jogalapja: a GDPR 6. cikk (1) bekezdés a) pontja szerinti érintetti hozzájárulás
Adattárolás határideje: a megüresedett pozíció betöltéséig
Adattárolás módja: elektronikusan
Érintetti jogosultságok: jelen szabályzat 6. fejezete szerint

15.2. Szerződésekkel és Számlázással Kapcsolatos Adatkezelés

(1) A Társaság megkötött szerződései tekintetében is figyelemmel van a GDPR-ban valamint az Infotv-ben rögzített adatvédelmi előírásokra, amelyből kifolyólag a Társaság azon szerződései tekintetében, amelyeket természetes személyekkel köt, vagy olyan jogi személyekkel vagy jogi személyiség nélküli gazdasági társaságokkal, ahol a szerződés teljesítése során egyéb közreműködő természetes személy nem vesz részt az adatkezelést a Társaság az alábbiak szerint végzi:
Adatkezelés célja: a szerződés teljesítése,
Kezelt adatok köre: a cégszerű képviseletre jogosult neve, a szerződésben megadott egyéb személyes adatai
Kezelt adatok forrása: közvetlenül az érintettől
Adatkezelés jogalapja: a GDPR 6. cikk (1) bekezdés b) pontja [szerződés teljesítése];
Adattárolás határideje: szerződés teljesítéséig, illetve a szerződés megszűnését követően a cégszerű képviselő személyes adatait a szerződésből eredő jogi igények érvényesítése és védelme céljából a Ptk. általános elévülési szabályai szerint, illetve a Számviteli törvényben a bizonylatok megőrzésére vonatkozó rendelkezések (8 év) szerint megőrzi a Társaság
Adattárolás módja: elektronikusan és papíralapon (amennyiben a megkötött szerződés papír alapú)
Érintetti jogosultságok: jelen szabályzat 6. fejezete szerint
(2) A Társaság azon szerződései tekintetében, amelyeket a Társaság olyan jogi személyekkel vagy jogi személyiség nélküli gazdasági társaságokkal köt, ahol a szerződés teljesítése során a szerződés teljesítésébe egyéb természetes személy közreműködő is bevonásra kerül a szerződő fél oldalán, a közreműködők személyes adataival kapcsolatos adatkezelést a Társaság az alábbiak szerint végzi:
Adatkezelés célja: a szerződés teljesítése illetve az ennek érdekében szükséges kapcsolattartás
Kezelt adatok köre: a kapcsolattartó neve, a szerződésben megadott egyéb személyes adatai
Kezelt adatok forrása: a szerződés

Adatkezelés jogalapja: a GDPR 6. cikk (1) bekezdés f) pontja [a Társaság jogos érdeke (szerződés teljesítése illetve az ennek érdekében szükséges kapcsolattartás]. Az érdekmérlegelési teszt a Társaság adatvédelmi tisztviselőjétől elektronikus úton kikérhető
Adattárolás határideje: szerződés teljesítéséig
Adattárolás módja: elektronikusan és papíralapon (amennyiben a megkötött szerződés papír alapú)
Érintetti jogosultságok: jelen szabályzat 6. fejezete szerint
(3) Azon szerződések tekintetében, amelyekhez kapcsolódóan a Társaság számlát fogad be és kifizetést teljesít, a Társaság a számlához kapcsolódó bizonylatokon lévő személyes adatok tekintetében z alábbi adatkezelési tevékenységet végzi:
Adatkezelés célja: a Társaság által befogadott számla kötelező adattartalmának megállapítása, a számlához kapcsolódó könyvviteli feladatok ellátása
Kezelt adatok köre: a számlán illetve ahhoz kapcsolódó bizonylatokon szereplő adatok
Adatkezelés jogalapja: a GDPR 6. cikk (1) bekezdés c) pontja szerinti jogi kötelezettség (2007. évi CXXVII. törvény 159. § (1) bekezdése illetve a 2000. évi C. törvény 169. § (1) bekezdése) teljesítése
Adattárolás határideje: a számviteli törvényben (169. § (1) bekezdés) rögzített határidőig (8 év)
Adattárolás módja: elektronikusan és papír alapon (amennyiben a számla papír alapon is rendelkezésre áll)
Érintetti jogosultságok: jelen szabályzat 6. fejezete szerint

15.3. A Társasággal Történő Kapcsolatfelvételhez Kapcsolódó Adatkezelés

A Társasággal kapcsolatot felvevő személyek által a kapcsolatfelvétel során megadott személyes adatokat a Társaság az alábbiak szerint kezeli:
Adatkezelés célja: a Társasággal kapcsolatot felvevő érintettekkel történő kapcsolattartás, kommunikáció
Kezelt adatok köre: az érintett neve, e-mail címe, telefonszáma, a kapcsolatfelvétel során az érintett által megadott egyéb személyes adat
Adatkezelés jogalapja: a GDPR 6. cikk (1) bekezdés a) pontja szerinti érintetti hozzájárulás
Adattárolás határideje: a hozzájárulás visszavonásáig. A hozzájárulás visszavonásának következménye, hogy a Társaság a hozzájárulás visszavonását követően nem fog tudni kapcsolatot tartani az érintettel. A hozzájárulás visszavonását megelőző adatkezelés jogszerűségét a hozzájárulás visszavonása nem érinti.
Adattárolás módja: elektronikusan
Érintetti jogosultságok: jelen szabályzat 6. fejezete szerint

15.4. Egészségügyi Adatokkal Kapcsolatos Adatkezelés

(1) A Társaság a GDPR-ban és az Infotv.-ben rögzített rendelkezéseken túlmenően a klinikai kutatás során az érintetti személyes és egészségügyi adatok kezelése során tiszteletben tartja az Eüak. törvényben foglaltakat is egyaránt, amely alapján a Társaság rögzíti, hogy az érintetti egészségügyi személyes adatokat az OMIII-val (mint vizsgálóhellyel) folyatott közös tudományos kutatás céljából kezeli összhangban az Eüak. 4. § (1) bekezdés d) pontjával.
(2) A klinikai kutatás során a klinikai vizsgálatokkal kapcsolatos elsődleges célból történő adatkezelést, azaz az érintettek vizsgálatát az OMIII végzi teljeskörűen, így a vizsgálathoz kapcsolódó betegtájékoztató részét képező adatkezelési tájékoztatót, illetve a vizsgálat lefolytatásához kapcsolódó beleegyező

nyilatkozatot az OMIII ismerteti meg és fogadtatja el a vizsgálati alannyal (érintettel) vagy törvényes képviselőjével. A Társaság a klinikai vizsgálatokhoz kapcsolódó másodlagos célból, azaz tudományos kutatás céljából kezeli a vizsgálati alanyok egészségügyi és az egészségügyi adatokhoz kapcsolódó személyes adatokat. A másodlagos célból folytatott adatkezelési tevékenységéről a Társaság részletes adatkezelési tájékoztatót készít, ismertet meg és fogadtat el az érintettekkel vagy törvényes képviselőjükkel.

(3) Az egészségügyi adatok kezelése tekintetében a Társaság tekintettel van a GDPR 9. cikkében rögzített, a személyes adatok különleges kategóriáinak kezelésére vonatkozó rendelkezésekre is, amelyek alapján az egészségügyi adatokat a Társaság az alábbiak szerint végzi:

Adatkezelés célja: a Neunos Zrt. Neunos SeizureSTOP™ NeuroClinical rendszerére, mint orvostechnikai eszközre vonatkozó, az Eüak. 4. § (1) bekezdésének d) pontjában rögzített tudományos klinikai kutatás eredményének kiértékelése és az eredményekről publikáció készítése

Kezelt egészségügyi adatok köre: MRI felvétel, EEG felvétel, vizsgálat során készített videofelvétel, gyógyszerezésre vonatkozó adat

Kezelt egészségügyi adatokhoz kapcsolódó személyes adatok köre: név, születési hely, idő, TAJ szám, vizsgálati alany anyja neve, lakcím

Kezelt adatok forrása: közvetlenül az érintettől, illetve hozzájárulásával az OMIII-tól

Adatkezelés jogalapja: az Eüak. 4. § (4) bekezdésében, GDPR 6. cikk (1) bekezdés a) pontjában és a GDPR 9. cikk (1) bekezdésében rögzített kifejezett érintetti hozzájárulás, továbbá a GDPR 6. cikk (1) bekezdés f) pontja, azaz a Társaság jogos érdeke, valamint ehhez kapcsolódóan a GDPR 9. cikk (i) és (j) pontja, azaz az, hogy az egészségügyi adatok kezelése olyan közérdekből szükséges mint az orvostechnikai eszközök magas színvonalának és biztonságának biztosítása illetve az, hogy az adatkezelés tudományos kutatási célból szükséges. Ezen túlmenően az Eüak. 4. § (2) bekezdés d) pontja, miszerint egészségügyi és személyazonosító adatot tudományos kutatás céljából kezelni lehet.

A fenti jogalapokból kifolyólag tekintettel arra, hogy a klinikai kutatás során megismert érintetti személyes és egészségügyi adatok kezelésével a Társaság célja az, hogy a klinikai kutatás eredményeit kiértékelje, illetve az, hogy az eredményekről tudományos publikációt készítsen és ebből a célból a kutatási eredményeket anonimizált módon felhasználja, az adatkezelés mind az érintettek önkéntes és kifejezett hozzájárulásával mind a Társaság jogos érdekére történő hivatkozással is egyaránt jogszerűen végezhető összhangban az Európai Adatvédelmi Testület 3/2019. sz. véleményével és az ETT KFEB klinikai vizsgálatokkal kapcsolatos ajánlásában foglaltakkal.

Adattárolás határideje: a kutatás lezárultától számított 5 év, illetve az érintett hozzájárulásának visszavonásáig. A hozzájárulás visszavonásának következménye, hogy a vizsgálati alany a továbbiakban nem tud részt venni a klinikai kutatásban a hozzájárulás visszavonását követően. A hozzájárulás visszavonását megelőző adatkezelés jogszerűségét a hozzájárulás visszavonása ugyanakkor nem érinti. A GDPR 17. cikk (3) bekezdés d) pontja értelmében a hozzájárulás visszavonására iránti kérelem teljesítése megtagadható, amennyiben az a tudományos kutatási célú adatkezelést nagy valószínűséggel lehetetlenné tenné vagy komolyan veszélyeztetné.

Adattárolás módja: elektronikusan

Adattovábbítás: az OMIII és a Társaság közötti adattovábbítás jogalapja a GDPR 6. cikk (1) bekezdésének b) pontjában rögzített, az OMIII és a Társaság között fennálló szerződés teljesítése. Ezen túlmenően az adattovábbítás további jogalapja a GDPR 6. cikk (1) bekezdés a) pontja szerinti és a GDPR 9. cikk (2) bekezdésének a) pontja szerinti érintetti hozzájárulás, valamint a GDPR 9. cikk (2) bekezdésének i) és j) pontjában foglaltak szerinti célok elérése (azaz az orvostechnikai eszközök magas színvonalának és biztonságának biztosítása és a tudományos kutatási cél).
EESZT-re történő adatfeltöltés: az OMIII a 39/2016. (XII.21.) EMMI rendelet értelmében köteles arra, hogy az Állami Egészségügyi Ellátó Központtal együttműködve az EESZT-be feltöltse a klinikai kutatáshoz kapcsolódó egészségügyi és ahhoz kapcsolódó személyes érintetti adatokat, megfelelve az Eüak.-ban foglaltaknak is egyaránt. (az EESZT-re vonatkozó adatkezelési tájékoztató itt érhető el: https://e-egeszsegugy.gov.hu/documents/26398/557047/EESZT_Lakossagi_adatkezelesi_tajekoztato_2021_v6.pdf/8678cf08-dbec-407d-03a9-f8e34e22fa43)
Érintetti jogosultságok: jelen szabályzat 6. fejezete szerint

15.5. Honlappal Kapcsolatos Adatkezelés

A Társaság saját honlappal rendelkezik: www.neunos.com
A Társaság által működtetett honlaphoz bárki, kiléte felfedése és személyes adatai megadása nélkül hozzáférhet, a honlapon és az ahhoz kapcsolt oldalakon szabadon és korlátozás nélkül szerezhet információkat. Nem személyhez kötött információkat azonban korlátlanul és automatikusan gyűjt a weblap a látogatókról. Ezekből az adatokból személyes adat azonban nem nyerhető, így a GDPR illetve Infotv. hatálya alá tartozó adatkezelést nem valósít meg.

16. Az Adatkezeléssel Kapcsolatos Érintetti Jogosultságok

16.1. Tájékoztatáshoz Való Jog

(1) Az érintett tájékoztatást kérhet arról, hogy a Társaság milyen személyes adatait kezeli, illetve a személyes adatai kezelésének körülményeiről a Társaság feltüntetett elérhetőségein.
(2) A Társaság az érintett személyes adatának kezelésével összefüggő kérelmére az érkezésétől számított legkésőbb 25 – tiltakozási jog gyakorlása esetén 15 – napon belül írásban, közérthető formában választ ad.
(3) A tájékoztatás kiterjed a GDPR 15. cikk (1) bekezdésében meghatározott információkra, amennyiben az érintett tájékoztatása törvény alapján nem tagadható meg. A Társaság megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó, a GDPR 13. és a 14. cikkben említett valamennyi információt és a GDPR 15–22. és 34. cikk szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.
(4) A tájékoztatás főszabály szerint ingyenes, költségtérítést a Társaság csak a GDPR 12. cikk (5) a) pontjában meghatározott esetben számíthat fel.

(5) A Társaság kérelmet csak a GDPR 12. cikk (5) bekezdés b) pontjában meghatározott okokból utasít el, erre csak indoklással, megfelelő tájékoztatással, írásban kerülhet sor.

16.2. Helyesbítéshez, Törléshez (Elfelejtéshez) Való Jog

(1) A valóságnak nem megfelelő adatot a Társaság – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, a GDPR 17. cikkében meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törlése iránt.
(2) Az érintett jogosult arra, hogy kérésére a Társaság indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, a Társaság pedig köteles arra – kivéve, ha jogszabály alapján a törlés iránti kérelmet jogosult elutasítani -, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, különösen ha az alábbi indokok valamelyike fennáll:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett visszavonja a hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- a személyes adatokat a Társaság jogellenesen kezelte.

16.3. Tiltakozás a Személyes Adatok Kezelésével Szemben

(1) Az érintett jogosult arra, hogy személyes adatai kezelése ellen bármikor tiltakozzon a Társasághoz intézett erre irányuló nyilatkozat útján, különösen, ha a személyes adatok kezelése vagy továbbítása kizárólag a Társaság jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén, valamint törvényben meghatározott egyéb esetben.
(2) Az érintett személyes adata kezelése elleni tiltakozásának elbírálásának időtartamára – de legfeljebb 5 napra – az adatkezelést a Társaság felfüggeszti, a tiltakozás megalapozottságát megvizsgálja és döntést hoz, amelyről a kérelmezőt a GDPR 19. cikk szerint tájékoztatja.
(3) Amennyiben a tiltakozás indokolt, a Társaság a GDPR 21. cikkében meghatározottak szerint jár el.
(4) Ha a Társaság az érintett tiltakozásának megalapozottságát megállapítja, az adatkezelést - beleértve a további adatfelvételt és adattovábbítást is – megszünteti, az adatokat zárolja, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.
(5) Ha az érintett a Társaság döntésével nem ért egyet, illetve, ha a Társaság a válaszadási határidőt elmulasztja, az érintett - a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül - bírósághoz fordulhat.
(6) A Társaság az érintett adatát nem törölheti, ha az adatkezelést törvény rendelte el.

16.4. Az Adatkezelés Korlátozásához Való Jog

Az érintett jogosult arra, hogy kérésére a Társaság korlátozza az adatkezelést, ha

- az érintett vitatja a személyes adatok pontosságát (ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Társaság ellenőrizze a személyes adatok pontosságát); vagy
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását; vagy
- a Társaságnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- az adatkezelés a Társaság vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, és az érintett tiltakozott az e célokból történő adatkezelés ellen (ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Társaság jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben).

16.5. Az Adathordozhatósághoz Való Jog

A Társaság jelen adatkezelési tájékoztatóban rögzített adatkezelési tevékenysége során nem valósul meg olyan adatkezelés, amely adathordozhatóság biztosítását tenné szükségessé.

16.6. Automatizált Döntéshozatal Egyedi Ügyekben, Beleértve a Profilalkotást

A Társaság jelen adatkezelési tájékoztatóban foglat adatkezelése során automatizált döntéshozatal, illetve profilalkotás nem valósul meg.

16.7. Jogellenes Adatkezeléssel Okozott Kár Megtérítéséhez Való Jog

A Társaság az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is megtéríti. A Társaság mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Ugyanígy nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

Jogorvoslathoz Való Jog

Az érintett jogorvoslati lehetőséggel, panasszal a Társaság adatvédelmi tisztviselőjéhez (Dr. Papp Viktória; dpo@neunos.com) fordulhat közvetlenül, vagy választása szerint a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (1055 Budapest, Falk Miksa utca 9-11; levelezési cím: 1363 Budapest, Pf. 9..) vagy lakóhelye vagy tartózkodási helye szerint illetékes törvényszékhez. A bírósági jogorvoslathoz való jogának érvényesítése érdekében az érintett a Társaság, illetve – az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint a Társaság, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli. A bíróság az ügyben soron kívül jár el.

_____

Gyurkovics Tamás
Neunos Zrt.
vezérigazgató

17. Mellékletek

1 sz. melléklet - Adatvédelmi hatásvizsgálat lefolytatásának szempontrendszere

18. Dokumentálás

Jelen szabályzattal kapcsolatos minden dokumentációt a Dokumentációkezelés minőségirányítási eljárásnak megfelelően kell elkészíteni, felülvizsgálni és jóváhagyni.

18.1. Dokumentumok Listája

- Data Breach Notification/Adatvédelmi Incidens bejelentő lap (NEU-TMP-085)

19. Referenciák

- **GDPR** – az Európai Parlament és Tanács (EU) 2016/679 számú rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (Általános Adatvédelmi Rendelet);
- **Infotv.** – az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;
- **Eüak.** – az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény;
- NEU-QM-008 Dokumentációkezelés

20. 1.sz. melléklet

Adatvédelmi hatásvizsgálat lefolytatásának szempontrendszere

A Társaság tevékenységének ellátásához kapcsolódóan az alábbi adatkezelési eljárást kívánja bevezetni, amelynek során a Társaság adatkezelőként jár el:

1. A bevezetni kívánt adatkezelési folyamat leírása:
2. Az adatkezelési műveletek módszeres leírása:
3. A Társaság és az adatkezelési folyamatban egyéb résztvevők megnevezése (a résztvevők státuszának és adatkezeléssel összefüggő tevékenységének leírása):
4. Az adatkezelés bevezetésének várható dátuma:

Az adatkezelés jogalapjának vizsgálata során az GDPR 6. cikk (1) bekezdése a)- f) pontjai irányadók.
Amennyiben a jogalapot a GDPR 6. cikk (1) bekezdés f) pontja jelenti: az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.
Az adatkezelés jogszerűségének vizsgálatához el kell végezni egy érdekmérlegelési tesztet, amelynek során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását kell vizsgálni és megfelelően alátámasztani.
A Társaság a GDPR 35. cikkének felhatalmazása alapján az alábbi hatásvizsgálatot végzi el:

1. **Az adatkezelés jogalapja**
2. **Az adatkezelés célja/az adatkezelő jogos érdekének leírása**

Az adatkezelés céljainak, indokainak leírása, különös tekintettel az adatkezelés szükségességének, elengedhetetlenségének alátámasztása:

1. **A kezelt adatok körének pontos meghatározása. Annak meghatározása, hogy az egyes adatok tekintetében fennáll-e az adatkezelési cél, az adat a cél elérésére alkalmas-e, szükséges-e?**
2. **Az érintettek köre**
3. **Az adatkezelés egyéb körülményei**
4. **Adattovábbítás körülményei (címzett, cél, jogalap)**
5. **Várható hatások, kockázatok**

Milyen lehetséges kockázatokkal jár az adatkezelés az érintettek jogainak esetleges sérelme szempontjából? Adatbiztonsági kockázatok vizsgálata. Az esetleges adatvesztések, jogosulatlan hozzáférések, vagy egyéb adatvédelmi incidensek bekövetkezésének lehetséges esetei, az incidens-bekövetkezés valószínűségének vizsgálata.

1. **Melyek az érintettek érdekei az adatkezeléssel kapcsolatban?** (Arányos-e az érintettek jogainak korlátozása az elérendő céllal? Csak annyiban korlátozza-e az érintettek jogait, amennyire a cél elérése érdekében szükséges?)
2. **Alternatíva keresése. Létezik-e más módszer a cél elérésére, amely az érintettek jogait kevésbé korlátozza? Ha létezik, ugyanolyan hatékonyan szolgálja-e a cél elérését?**

3. **A kockázatok elhárítására tett intézkedések, garanciák, a felek együttműködése**
4. **A megtett intézkedések leírása.** (Az egyes intézkedések mennyiben csökkentik az adatkezelési kockázatokat. Adatbiztonsági intézkedések leírása (fizikai, logikai, adminisztratív intézkedések megtétele).
5. **Az érintettekkel való együttműködés biztosítása** (jogorvoslati lehetőségek, kérelemre történő tájékoztatásadás lehetősége, adatvédelmi szabályzat megléte, adatvédelmi tisztviselő kinevezése, stb.).
6. **A hatásvizsgálat eredményének megállapítása** (a kockázat mértékének, jellegének leírása, további intézkedések megtételének szükségessége, előzetes konzultáció szükségessége, a kockázat mértékének, jellegének leírása, következtetés levonása (miért jogszerű az adatkezelés, miért fűződik magasabb érdek a cél eléréséhez, illetve az érintettek jogainak korlátozása mitől arányos).
7. **Érintettek jogainak leírása, tiltakozás, hozzáférhetőség joga**