

Data protection and data management policy

1.) Purpose of data management

Dr. Róbert Ligetfalvi, as a data controller (hereinafter referred to as data controller), acknowledges the content of these regulations as binding on him. The data controller undertakes that all data processing related to his activities complies with the provisions of these regulations, domestic legislation and legal acts issued by the European Union.

The data controller respects the right of informational self-determination of its clients and is committed to protecting the personal data of its clients. The data controller declares and undertakes to treat the personal data and health data obtained by him as confidential, and to take all technical, organizational and security measures that guarantee the safety of data management and preservation.

2.) The data of the data controller

If you have any questions about data management, you can ask them at the contact details below:

Name: MAMMA RAD Kft.

Registered office: HU-4400 Nyíregyháza Sólyom utca 27 1/ 1.

Company registration number: 15-09-089996

VAT number: 27850080-1-15

Telephone number: +36308686241

E-mail: info@preventivescan.hu

3.) Scope of processed personal data:

3.1.) Technical data

The data controller selects and operates the IT tools used for the management of personal data during the provision of the service in such a way that the processed personal data:

- be available to the persons entitled to it (availability),
- their authenticity and authentication be ensured (authenticity of data management),
- their immutability can be verified (data integrity),
- be protected against unauthorized access (data confidentiality).

The data controller protects personal data against unauthorized access, change, transmission, disclosure, deletion, destruction, and accidental destruction with appropriate measures.

The data controller ensures the protection of the security of data management with such technical, structural and organizational measures that provide a level of protection corresponding to the risks associated with data management.

During processing personal data, the data controller preserves

- confidentiality: he protects the information so that it could be available only by the authorized persons,
- integrity: he protects the accuracy and completeness of the information and the method of processing,
- availability: he ensures that when the authorized user needs it, he/she can really access the desired data and that the related tools are available.

4.) Purpose, method and legal ground of data management

The purpose of handling health and personal identification data:

- a) promoting the preservation, improvement and maintenance of health,*
- b) facilitating the effective medical treatment activities of the patient care provider, including also professional supervision,*
- c) monitoring the health status of the person concerned,*
- d) taking the measures that become necessary in the interest of national health, public health and epidemiology*
- e) enforcement of patient rights,*
- f) tracking the individual patient history,*
- g) follow-up of the human reproduction procedure, assessment of the medical effectiveness of the procedure and, based on this, the medical quality of the human reproduction procedures, review and development of the aspects of the evaluation.*

5.) Data management for the purpose of medical treatment

5.1.) The data controller and the data processor are obliged to maintain medical confidentiality.

The data controller is exempt from the obligation of secrecy if

- the data subject or his/her legal representative has consented in writing to the transfer of health and personal identification data, within the limitations contained therein, and
- the transfer of health and personal identification data is mandatory according to the law.

The data subject shall be charged a fee for each additional copy of the personal data subject to data management as defined in paragraph (3) of article 15 of Regulation (EU) 2016/679 of the European Parliament and Council (hereinafter referred to as General Data Protection Regulation) on the basis of the cost elements specified in the Ministerial Decree.

This right belongs to

- the person authorized by the data subject in writing during the period of his/her care,
- after the end of the care of the data subject, it belongs to the person authorized by him/her in a private document with full evidential force.

During the patient's lifetime, or after his/her death, the spouse, lineal relative, sibling, and partner in life of the data subject - based on their written request - are also entitled to exercise the above-mentioned right if

- a) the health data is necessary*
 - aa) for the purpose of disclosing a cause influencing the life, health of the spouse, lineal relative, sibling, and partner in life as well as their descendants or*
 - ab) for the purpose of the medical attendance of the persons as per point aa) and*

b) it is not possible to get to know the health data in any other way or to draw conclusions about it.

5.2.) The patient care provider is also bound by the obligation of secrecy vis-à-vis the patient care provider who did not cooperate in the medical examination, diagnosis, medical treatment or surgery, except if the disclosure of the data is necessary for the diagnosis of the disease or for the further medical treatment of the data subject.

5.3.) The recording of health data is a part of medical treatment. The treating doctor or the medical officer decides which medical data needs to be recorded in accordance with the professional rules, in addition to the mandatory data.

Other persons carrying out activities related to the medical treatment of the data subject may record health data in accordance with the instructions of the doctor performing the treatment, or to the extent necessary for the performance of their duties.

6.) Data transfer, circle of people getting to know health data

6.1.) In the case of data management and data processing, health and personal identification data can be transmitted or connected within the health care network. In order to perform duties determined in §81 of Act LXXXIII of 1997 (hereinafter referred to as Ebtv.) on the compulsory health insurance benefits of the health insurance body health data and social security numbers (hereinafter referred to as SSN) can be transmitted or connected between the health care network and the health insurance body, to the extent necessary for the performance of the duty. Health and personal identification data from different sources can only be linked up to the time and to the extent absolutely necessary for prevention, medical treatment, national health, public health-epidemiological measures.

6.2.) All health data related to the data subject's illness may be forwarded, which, based on the decision of the attending physician or family doctor, is important for medical treatment, except if the data subject prohibits this in writing or in a self-determination registered statement. The data subject must be informed of this possibility before the transfer.

6.3.) Even in the case of data transmission, health data relating to a previous illness unrelated to the illness existing at the time of transmission may not be forwarded without the consent of the data subject.

6.4.) In the event of an urgent need, all medical and personal identification data known to the treating physician and related to the medical treatment can be forwarded.

6.5.) The treating physician directly informs the data subject about the health data he/she has established regarding the data subject and - if the data subject has not expressly prohibited this - forwards them to the data subject's chosen family doctor.

6.6.) The family doctor of the data subject and the doctor treating him/her - if the data subject has not prohibited this in writing - are entitled to learn about the health care data used by the data subject at the expense of the compulsory health insurance, in such a manner that the health insurance body provide the data to them in the form of electronic inquiry. The doctor performing the treatment informs the data subject in writing or orally about the possibility of protest. The data subject shall submit his/her protest to the health insurance body in person, by post or electronically.

6.7.) The authorization for individual data viewing and data management does not entitle the attending physician either to pass on the data or to use them for other purposes.

6.8.) In the event that the data subject voluntarily applies to the health care network, his/her consent to the handling of his/her medical and personal identification data related to medical treatment shall be deemed to have been given – in the absence of a statement to the contrary – and the data subject (his/her legal representative) shall be informed of this. Voluntariness must be assumed in the case of an urgent need, as well as in the case of the data subject's lack of discretion.

6.9.) During the medical treatment, apart from the treating doctor and other patient care persons, only those may be present to whose presence the data subject consents. The following persons can be present without the consent of the data subject, respecting the human rights and dignity of the data subject:

- a)* another person, if the order of medical treatment requires the simultaneous care of several patients,
- b)* a professional member of the police, if medical treatment is carried out in the case of a detained person,
- c)* a member of the penal institution in a service relationship, if the medical treatment is carried out in the case of a person who is serving a sentence involving deprivation of liberty in the penal institution, and this is necessary for the safety of the person providing the medical treatment, or to prevent escape,
- d)* persons according to points *b)-c)* if the personal safety of the patient justifies this in the interests of law enforcement and the patient is unable to make a statement.

In addition to the persons defined above, the following persons may be present without the consent of the data subject:

- a)* who previously treated the data subject for the given disease,
- b)* to whom the head of the institution or the data protection officer has given permission for professional and scientific purposes, except if the data subject has expressly objected to this.

6.10.) When ordering medicine, medical aids and medical care, the following must be indicated on the prescription:

- a)* name, address and date of birth of the data subject,
- b)* in the case of a prescription with social security support, in addition to the provisions in point *a)*, the social security number of the data subject, the code of his/her illness according to the International Classification of Diseases (BNO code) and
- c)* in the case of a patient receiving public medical care, in addition to the provisions in points *a)* and *b)*, the number of the public medical care card,
- d)* in the case of prescriptions ordered through the Electronic Health Services Area (hereafter referred to as EESZT), in addition to what is contained in points *a)-c)*, the gender of the data subject, in addition to this the social security number of the data subject, or, in the absence of this, the number of another document suitable for personal identification used to identify the data subject.

6.11.) The health and personal identification data collected from the data subject and necessary for medical treatment, as well as their transmission, must be recorded. The record of data transmission must include the recipient, the method, the date of the data transmission, as well as the scope of the data transmitted.

The means of record can be any data storage device or method that ensures data protection.

6.12.) The treating physician makes a record of the health data recorded by him or other persons providing medical attendance, as well as his own activities and measures related to it. The note forms a part of the record.

7.) Data retention period

7.1.) The health documentation - with the exception of the images taken with the imaging diagnostic procedure and the findings made about it - must be kept for at least 30 years from the date of data collection, and the final report for at least 50 years. After the mandatory registration period, the data can still be registered for medical treatment or scientific research - if justified. If further registration is not justified, the records must be destroyed.

7.2.) A recording made with an imaging diagnostic procedure must be kept for 10 years from the date it was taken, and the findings from the recording must be kept for 30 years from the date the recording was made.

7.3.) If the medical documentation is of scientific importance, it must be handed over to the competent archive after the mandatory registration period.

7.4.) In the event of the termination of the documentation manager without a legal successor
a) medical documentation of scientific importance must be handed over to the archive,
b) other health documentation must be handed over to the body designated by the Government.

7.5.) Incorrect medical data contained in the medical documentation must be corrected or deleted after the data has been collected so that the originally recorded data can be established. The data controller shall make a certified copy of the registered data and health documentation if this is necessary for data security or the physical protection of the stored data, or the data disclosure obligation prescribed by this law.

8.) General data management guidelines

Our data management principles are in line with the applicable data protection legislation, in particular the following:

- *Act CXII of 2011 on the right to informational self-determination and freedom of information (Infotv.),*
- *The decree of the European Parliament and Council no. (EU) 2016/679. (27 April, 2016) on the protection of natural persons with regard to the processing of personal data and the free flow of such data as well as the repeal of the Decree no. 95/46/EC (GDPR),*
- *Act V of 2013 on the Civil Code (Ptk.),*
- *Act XLVII of 1997 on the handling and protection of health data and related personal data*

9.) The physical storage locations of the data

Health data obtained during the health care service are recorded in the Data Controller's storage space, to which only the data controller and the person authorized by him have access.

10.) Rights and remedies of the data subject

The data subject:

- can request information about the management of his/her personal data,
- can request correction of his/her personal data,
- can request the deletion of his/her personal data,
- can request the withdrawal of his/her personal data,
- can use his/her data portability and objection rights.

10.1.) Right to information

The data controller takes appropriate measures in order to provide the data subjects with all the information mentioned in articles 13 and 14 of the GDPR and as per articles 15-22 and article 34 regarding the processing of personal data in a brief, transparent, comprehensible and easily accessible form, clearly and comprehensibly worded.

10.2.) The data subject's right of access

The data subject has the right to receive feedback from the data controller as to whether his/her personal data is being processed, and if such data processing is in course, he/she is entitled to access personal data and the following information:

- the purposes of data management,
- categories of personal data concerned,
- recipients or categories of recipients to whom or to which the personal data has been or will be communicated,
- the planned period of storage of personal data,
- the right to rectification, deletion or restriction of data processing and the right to object,
- the right to submit a complaint to the supervisory authority,
- information about data sources,
- the fact of automated decision-making, including profiling,
- information about the applied logic and the significance of such data management and the expected consequences for the data subject.

The data controller shall provide the information within a maximum of one month from the date of submission of the request.

10.3.) Right to rectification

The data subject may request the correction of inaccurate personal data concerning him/her managed by the data controller and the addition of incomplete data.

10.4.) Right to deletion

If one of the following reasons exists, the data subject is entitled to have the data controller delete the personal data relating to him/her without undue delay:

- personal data are no longer needed for the purpose for which they were collected or otherwise processed,

- the data subject withdraws his/her consent, which is the basis of the data management, and there is no other legal ground for the data management,
- the data subject objects to the data processing and there is no overriding legal reason for the data processing,
- personal data were handled illegally,
- personal data must be deleted in order to fulfil a legal obligation prescribed by EU or member state law applicable to the data controller,
- the collection of personal data took place in connection with the offering of services related to the information society.

Data deletion cannot be initiated if data management is necessary:

- for the purpose of exercising the right to freedom of expression of opinion and information,
- for the purpose of fulfilling an obligation according to the EU or member state law applicable to the data controller requiring the processing of personal data, or for the execution of a task carried out in the public interest or in the context of the exercise of public authority conferred on the data controller,
- for a purpose affecting the field of national health or for archival, scientific and historical research purposes or for statistical purposes, based on public interest,
- for the submission, enforcement and defence of legal claims.

10.5.) The right to restrict data processing

At the request of the data subject, the data controller restricts data processing if any of the following conditions is met:

- the data subject disputes the accuracy of the personal data, in this case the restriction applies to the period that allows the checking of the accuracy of the personal data,
- the data processing is illegal, and the data subject objects to the deletion of the data and instead of this he/she requests the restriction of their use,
- the data controller no longer needs the personal data for the purpose of data management, but the data subject requires them for the submission, enforcement or defence of legal claims,
- the data subject objected to the data processing; in this case the restriction applies to the period until it is determined whether the legitimate reasons of the data controller take precedence over the legitimate reasons of the data subject.

If the data management is subject to restriction, the personal data, with the exception of storage, can only be handled with the consent of the data subject, either for the submission, enforcement or defence of his/her legal claim or for the protection of the rights of any other natural or legal entity or for an important public interest of the EU or any other member state.

10.6.) Right to data portability

The data subject has the right to receive the personal data concerning him/her provided to the data controller by him/her in a segmented, widely used, machine-readable format, and to forward these data to another data controller.

10.7.) Right to protest

The data subject has the right to protest at any time for reasons related to his/her own situation against the processing of his/her personal data necessary for the performance of a task carried out in the public interest or within the framework of the exercise of public authority granted to the data controller, or for the enforcement of the lawful interests of the data controller or a third party, including profiling based on the aforementioned provisions as well.

In the event of a protest, the data controller may no longer process the personal data, unless it is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are related to the submission, enforcement or defence of legal claims.

10.8.) Automated decision-making in individual cases, including profiling

The data subject has the right not to be covered by the scope of a decision based solely on automated data management, including profiling, which would have a legal effect on him/her or would affect him/her to a similarly significant extent.

10.9.) Right of withdrawal

The data subject has the right to withdraw his/her consent at any time.

10.10.) Right to go to court

In the event of a violation of his/her rights, the data subject may apply to the court against the data controller. The court acts out of sequence in the case.

10.11.) Data protection official procedure

You can file a complaint to the Hungarian National Authority for Data Protection and Freedom of Information.

Name: Hungarian National Authority for Data Protection and Freedom of Information

Registered office: HU-1055 Budapest, Falk Miksa utca 9-11.

Mailing address: HU-1363 Budapest, Pf.: 9.

Telephone: +36 30 683 5969, +36 30 549 6838, +36 1 391 1400

Fax: +36 1 391 1410

E-mail: ugyfelszolgalat@naih.hu

Webpage: <http://www.naih.hu>

11.) Other provisions

We provide information on data management not listed in this information when the data is collected. We also inform our clients that the court, the prosecutor's office, the investigative authority, the infringement authority, the public administrative authority, the Hungarian National Authority for Data Protection and Freedom of Information, the Hungarian National Bank, or other bodies based on the authorization of the law, may can contact the data controller in order to provide information, communicate, transfer data or making documents available.

If the authority has indicated the exact purpose and the scope of the data, the data controller will only release personal data to the authorities to the extent that is absolutely necessary to achieve the purpose of the request.