Az Országos Foglalkozás-Egészségügyi Szolgálat
Limited Liability Company
General Data Processing Policy

1. Goal

This Policy sets out the data processing regime, the general rules and certain specific rules applicable to the processing of personal data carried out by the Országos Foglalkozás-Egészségügyi Szolgálat Korlátolt Felelősségű Társaság (hereinafter referred to collectively as OFESZ), subject to the provisions of Regulation 2016/679 of the European Parliament and of the Council (hereinafter referred to as the Regulation or GDPR).
This Policy does not cover, in addition to the general provisions contained therein, the processing of data relating to OFESZ employees and any other processing governed by specific rules.

2. Area of validity, scope and availability of the Code

The entire territory of the OFESZ.
The scope and general provisions of this Policy apply to all processing of personal data by the OFESZ and to all OFESZ employees.
This Policy is available and may be consulted by any person at the headquarters of the OFESZ. The OFESZ shall make this Policy available to persons who have or wish to have a contractual relationship with it and shall draw their attention to it.

DATA CONTROLLER AND PROCESSOR:

Országos Foglalkozás-Egészségügyi Szolgálat Kft.

Registered office: 2724 Újlengyel, Határ út 12.
Company registration number: 13-09-165927
Tax number: 11859059-2-13
Internet address: www.hivataloscovidteszt.hu
Email: teszt@hivataloscovidteszt.hu

Details of the hosting provider:

Contabo GmbH

Aschauer Straße 32a
81549 Munich
Germany

Phone.: + 49 (0) 89 212 683 72
Fax.: +49 (0) 89 216 658 62

revocation@contabo.com

This privacy statement governs the processing of data on the website www.hivataloscovidteszt.hu and is based on the content of the above mentioned content.

It is available at: www.hivataloscovidteszt.hu

Amendments to the Prospectus will enter into force upon publication at the above address.

3. Policy

3.1. Privacy policy

In its activities, the OFESZ takes great care to comply with the following key guidelines of the Regulation in order to protect personal data:

- the OFESZ processes data lawfully and fairly and in a transparent manner for the data subject (principles of legality, fairness and transparency);
- the OFESZ processes data only for specified, explicit and legitimate purposes (purpose limitation principle);
- the OFESZ processes only the data strictly necessary for the purposes of the processing (data minimisation principle);
- the OFESZ will promptly delete or rectify any personal data that are inaccurate for the purposes for which they are processed (accuracy principle);
- the OFESZ stores the data only for the time necessary to achieve the purposes for which it is processed (principle of limited retention);
- the OFESZ processes the data in such a way as to ensure the security (integrity and confidentiality) of the personal data by implementing appropriate technical or organisational measures.

a) The OFESZ processes personal data with the consent of the data subject or within the scope specified by law or, on the basis of the law's authorisation, within the scope specified therein, by local government regulation. The data subject's consent shall be deemed to be given if, when contacting the OFESZ, he or she is informed of the circumstances and facts of the processing and consents to the processing. Consent may also be given through an implied act, depending on the situation.

   As a general rule, the OFESZ will only process sensitive data if the data subject explicitly consents to the processing or, in certain specific cases, if it is necessary for the implementation of an international treaty proclaimed by law or if it is required by law for the exercise of a fundamental right guaranteed by the Fundamental Law, for the purposes of national security, the prevention or prosecution of criminal offences or in the interests of national defence, or if the processing is necessary for the fulfilment of other legal obligations to which the OFESZ is subject. However, the OFESZ does not process data revealing racial or ethnic origin, political opinions or political party affiliations, religious or philosophical beliefs or similar data under any circumstances.

b) The OFESZ may also process personal data where the processing is necessary for the purposes of the legitimate interests pursued by the OFESZ or by a third party and the pursuit of those interests is proportionate to the restriction of the right to the protection of personal data.

c) The OFESZ may also process personal data where the data subject is incapacitated or otherwise unable to give his or her consent and the processing is necessary for the protection of the vital interests of a person or for the prevention or elimination of an imminent threat to the life, physical integrity or property of a person.

d) The OFESZ processes the data it handles in strict compliance with the purpose

limitation principle. Accordingly, it processes personal data only for specified purposes, for the exercise of a right or the performance of an obligation, and at all stages of its processing it complies with that purpose. The OFESZ only processes personal data that is necessary for the purposes for which it is processed. The processing of personal data shall start on the date on which the legal relationship with the data subject begins and shall continue for the time necessary to achieve the purposes of the processing and to ensure legal compliance.

e) In all cases where the collection, processing or recording of data is not required by law, the OFESZ reminds the user of the voluntary nature of the data provision.

f) In all cases where OFESZ intends to use the data provided for purposes other than those for which they were originally collected, OFESZ will inform the data subject and obtain his or her prior explicit consent or give him or her the opportunity to object to such use.

4. Definitions of terms

For the purposes of the provisions of this Policy in relation to the processing of data by the OFESZ, the terms listed below shall have the following definitions:

data controller: a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by Union or Member State law, the controller or the specific criteria for the controller's designation may also be determined by Union or Member State law;

data management: any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, ttransfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

data processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

personal data: any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

special data: personal data revealing racial or ethnic origin, nationality, political opinions or opinions, religious or philosophical beliefs, membership of an interest group, sex life, health, pathological or mental disorder and personal data concerning criminal offences;

contribution: a voluntary and explicit indication of the data subject's wishes, based on appropriate information, by which he or she gives his or her unambiguous consent to the processing of personal data concerning him or her, whether in full or in part;

objection: a statement by the data subject objecting to the processing of his or her personal data and requesting the cessation of the processing or the erasure of the processed data;

data transfer: making the data available to a specified third party;

disclosure to the public: making the data available to anyone;

erasure: making data unrecognisable so that it is no longer possible to recover it;

data marking: the marking of data with an identification mark to distinguish it;
data blocking: the marking of data with an identification mark for the purpose of limiting their further processing permanently or for a limited period of time;
data destruction: the total physical destruction of a data medium containing data;
processing: the performance of technical tasks related to data processing operations, irrespective of the method and means used to carry out the operations and the place of application, provided that the technical task is performed on the data;
processor: a natural or legal person or an unincorporated body which, under a contract with a controller, including a contract entered into pursuant to a legal provision, processes data;
data controller: the public sector body which has produced the data of public interest which must be made public by electronic means or in the course of whose activities the data were generated;
data provider: the public sector body which, if the data controller does not publish the data itself, publishes on a website the data supplied to it by the data controller;
data set: the set of data managed in a register;
third party: a natural or legal person or unincorporated body other than the data subject, the controller or the processor.
Data Subject/User: any natural person who is identified or can be identified, directly or indirectly, on the basis of specific personal data;
personal health data: data concerning the health of the data subject which contain information about the past, present or future physical or mental health of the data subject. This includes:
registration for health services;
a number, symbol or data assigned to a natural person for the purpose of identifying that person individually for health purposes;
information derived from the testing or examination of a body part or body constituent, including genetic data and biological samples;
information relating to the illness, disability, disease risk, medical history, clinical treatment or physiological or biomedical condition of the data subject, irrespective of its source, which may be, for example, a doctor or other health professional, a hospital, a medical device or a diagnostic test.
genetic data: shall be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person and which are the result of the analysis of a biological sample taken from that person, in particular chromosomal analysis or analysis of deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) or any other element allowing the extraction of information equivalent to that which may be obtained from them.
alias: the processing of personal data in such a way that it is no longer possible to identify the natural person to whom the personal data relate without further information, provided that such further information is kept separately and technical and organisational measures are taken to ensure that no association with identified or identifiable natural persons is possible;
registration system: a set of personal data, disaggregated by any means, centralised, decentralised or by functional or geographical criteria, which is accessible on the basis of specific criteria;
data breaches: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Act XLVII of 1997 on the processing and protection of personal data concerning health and related matters:

health data: any data relating to the physical, mental or psychological state, pathological condition or addiction of the person concerned, the circumstances of the illness or death, the cause of death, as communicated by him or her or by another person, or as observed, tested, measured, mapped or derived by the healthcare network; and any data relating to or affecting any of the foregoing (e.g. behaviour, environment, occupation);

personal identification data: the surname and given name, maiden name, sex, date and place of birth, mother's maiden name and given name, place of residence, place of stay, social security number (hereinafter referred to as "social security number"), or any of these, together, where they are or may be capable of identifying the data subject;

medical treatment: any activity aimed at the preservation of health and the direct examination, treatment, care, medical rehabilitation or processing of the examination material of a person concerned for the purpose of preventing, detecting, diagnosing, treating, maintaining or correcting a disease, including the supply of medicines, medical aids, medical care, rescue and ambulance services and obstetric care;

medical secret: medical and personal data that have come to the knowledge of the controller in the course of treatment, as well as other data relating to necessary or ongoing treatment or treatment that has been completed, and other data obtained in connection with the treatment;

medical documentation: a record, register or any other form of information, regardless of its medium or form, containing medical and personal data, which comes to the attention of the healthcare provider in the course of treatment;

attending physician: the attending physician within the meaning of point b) of § 3 of the Eütv;

patient care: the physician, the healthcare professional, the other person involved in the treatment of the person concerned, the pharmacist;

data controller: a natural or legal person or unincorporated organisation that is entitled to process health and related personal or identity data for the purposes of data processing under this Act;

close relative: a spouse, a relative in the direct line, an adopted child, a stepchild, a foster child, an adoptive parent, a foster parent, a step-parent, a brother or sister and a life partner;

urgent need: a sudden change in health which, in the absence of immediate medical attention, would place the person in immediate danger of death or serious or permanent impairment of health

EEA country: a Member State of the European Union and another State party to the Agreement on the European Economic Area, and a State whose nationals enjoy the same status as nationals of a State party to the Agreement on the European Economic Area under an international treaty concluded between the European Community and its Member States and a State not party to the Agreement on the European Economic Area;

third country: any state that is not an EEA state;

Data management policies

- The processing of personal data must be lawful, fair and transparent for the data subject.
- Personal data shall be collected only for specified, explicit and legitimate purposes.

- The purposes for which personal data are processed must be adequate, relevant and limited to what is necessary.
- Personal data must be accurate and kept up to date. Inaccurate personal data must be deleted without delay.
- Personal data must be stored in a form which permits identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods only if the storage is for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes.
- Personal data shall be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by appropriate technical or organisational measures.
- The principles of data protection shall apply to any information relating to an identified or identifiable natural person.
- An employee of the organisation who is responsible for data processing shall be liable to disciplinary action, compensation, civil and criminal liability for the lawful processing of personal data. If an employee becomes aware that personal data he or she is processing is inaccurate, incomplete or out of date, he or she shall correct it or have it corrected by the person responsible for recording it.

4.1. Scope of data processed, specific rules for data management

The OFESZ carries out several types of data processing in the course of its activities. In this chapter, the OFESZ identifies the processing of personal data that is generally applicable to the OFESZ.
In addition to those listed in this Chapter, OFESZ may also process data in accordance with the provisions of specific regulations or data for which no specific regulations have been published but for which OFESZ has obtained the consent of the data subjects or otherwise has a legitimate interest which can be justified.
In processing data not covered by this Chapter, the OFESZ shall apply the relevant provisions of the Regulation and the general provisions of this Code mutatis mutandis.

Guidelines for the processing of health and related personal data:

*The provisions of the Health Care Act shall apply to all organisations and natural persons providing health care and performing professional supervision and control thereof (hereinafter referred to as "**health care network**"), as well as to all legal persons, organisations without legal personality and natural persons processing health and personal data (hereinafter referred to as "**other data controller**").*
*The Health Care Act shall also apply to any natural person, whether sick or healthy (hereinafter referred to as '**the data subject**'), who has come into contact with or is in contact with the health care network and the other data controllers or who uses their services, as well as to health and personal data relating to the data subject processed in accordance with the provisions of the Health Care Act.*
Personal data may be processed only in cases and to the extent necessary for the fulfilment of a legitimate purpose.

Purpose of processing health and personal data:
- to promote the preservation, improvement and maintenance of health,
- to monitor the health status of the data subject,

- to take measures necessary in the interests of public health, public health and epidemiology,
- enforce patients' rights.
- medical and epidemiological investigation, analysis, planning, organisation and costing of health care,
- statistical analysis,
- facilitating the work of bodies carrying out official or statutory controls, professional or statutory supervision of bodies or persons handling health data, where the purpose of such controls cannot be achieved by other means, and the tasks of bodies financing health care,
- the award of social security or social benefits, where this is based on health status,
- the assessment of fitness for work, whether such activity is carried out in the context of an employment relationship, a civil service, government service, public service, public service, professional service or other legal relationship,
- for the continuous and safe supply of prescribed medicines, medical appliances and medical care to persons entitled to health care,
- the ethical conduct of healthcare workers,
- determining the effectiveness of medicines and medical devices receiving performance-based reimbursement and the reimbursement of such medicines and establishing the funding procedures for the treatment of such conditions,
- organisation of patient journeys,
- evaluation and improvement of the quality of health services, regular review and improvement of the evaluation criteria for health services,
- monitoring, measuring and evaluating the performance of the health system,

The processing of health and personal data for purposes other than those listed above is also permitted by the legislator (e.g. sending newsletters, website registration, etc.) with the written informed consent of the data subject or his or her legal or authorised representative (hereinafter together referred to as "legal representative").

Records of health and identity data, processing of personal data

The medical and personal data recorded on the data subject which are necessary for the purposes of the investigation, and their transfer, must be recorded. The record of the transfer must include the recipient, the means, the date and the scope of the data transferred. The means of recording may be any data storage device or method that ensures the protection of data in accordance with § 6 of the Health and Safety at Work Act. The testing physician shall keep a record of the medical data recorded by him or by the other patient care provider and of his own activities and actions in connection therewith. The record shall form part of the register.
An erroneous medical record in the medical record shall be corrected or deleted after the record has been made in such a way that the original record can be identified.

Within the health care institution, the head of the institution handling the data is responsible for the protection of health and personal data and for the preservation of the records.

Since the natural persons concerned can be linked to online identifiers provided by the devices, applications, tools and protocols they use, such as IP addresses and cookie identifiers, this data, when combined with other information, can and may be used to create a profile of the natural persons and to identify that person. OFESZ does not perform profiling when processing health and related personal data.

Processing may take place only and exclusively where the data subject gives his or her freely given, specific, informed and unambiguous consent to the processing of the data by means of a clear affirmative action, such as a written, including electronic, or oral statement.

Consent to the processing shall also be deemed to be given when the data subject ticks a box when browsing the website (e.g. subscribing to a newsletter), when a user makes technical settings when using electronic services, or when he or she makes a statement or action which unambiguously indicates the data subject's consent to the processing of his or her personal data in that context.

Silence, ticking a box or inaction does not constitute consent.

Personal data shall be processed in a manner that ensures an adequate level of security and confidentiality, inter alia, to prevent unauthorised access to and use of personal data and the means used to process personal data.

Personal data of children are particularly protected.

apply to the use of children's personal data for marketing purposes or for the purpose of creating personal or user profiles.

All reasonable steps will be taken to correct or delete inaccurate personal data upon request of the data subject.

Where the data subject gives his or her consent in a written statement which also relates to other matters, the request for consent must be communicated in a manner clearly distinguishable from those other matters.
The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent prior to its withdrawal. The data subject shall be informed before consent is given. The withdrawal of consent shall be made possible in the same simple manner as the giving of consent.
In the case of children under the age of 16, the processing of personal data of children is lawful only if and to the extent that consent has been given or authorised by the person having parental authority over the child.

The principle of fair and transparent processing requires that the data subject be informed of the fact and purposes of the processing.

The data subject should have the right of access to the data collected concerning him or her and the right to exercise that right simply and at reasonable intervals in order to ascertain and verify the lawfulness of the processing. Each data subject should have the right to be informed, in particular, of the purposes for which personal data

are processed and, where possible, of the period for which the personal data are processed.

In particular, the data subject has the right to have his or her personal data erased and no longer processed if the collection or other processing of the personal data is no longer necessary in relation to the original purposes of the processing or if the data subjects have withdrawn their consent to the processing of the data. Health and related personal data cannot be deleted at such an address, as the controller is required by law to retain such data.

Where personal data are processed for direct marketing purposes, the data subject should have the right to object, free of charge and at any time, to the processing of personal data relating to him or her for such purposes.

In order to ensure that the storage of personal data is limited to the period necessary, the controller shall set time limits for erasure or periodic review, with a periodic review period set by the head of the organisation: 2 years

The controller has the obligation to implement appropriate and effective measures and to be able to demonstrate that the processing activities comply with the applicable legislation. (accountability principle)

4.1.1. Business partner data management

OFESZ collects and processes the personal data of its business partners (hereinafter referred to as "partner") to the extent necessary for the cooperation with the partner. The purpose of data processing is to carry out the business activities of OFESZ, to maintain contact and to enforce claims and recover debts arising in this context. The processing shall be limited to what is necessary for the purposes set out herein and shall at all stages be compatible with the purposes set out herein. If the purpose of the processing is fulfilled or ceases to exist, the personal data shall be deleted without delay.
The OFESZ generally manages the partner

- name,
- your registered office
- your tax number,
- account number,
- name of your representative,
- name of contact person, telephone number, email address.

The use of OFESZ's own internal system as a customer database will help achieve the objectives set out in the OFESZ business strategy. The database provides the OFESZ with a repository of information on current and potential partners. Personal data relating to current and potential partners will be stored in the database if the OFESZ has obtained the data subject's consent to the storage of the data after having informed the data subject.

4.1.2. Telephone call data management

a. The OFESZ is entitled to request data (call logs) from telecommunications service providers about the call data of mobile phones subscribed to by the OFESZ, and to manage and process these data, provided that there is a legal basis for doing so. The purpose of the processing is to ensure effective protection against possible security

threats to OFESZ and to ensure strategic cost analysis.

b. OFESZ does not record conversations on the landline phones it uses or the mobile phones it subscribes to.

4.1.3. Visitor data management

a. In the case of a person seeking to do business with the OFESZ, consent to the processing should be presumed.
b. Data on visitors to the OFESZ headquarters may be collected and processed by authorised OFESZ employees.
c. The following visitor data can be registered:
   – name
   – the name and registered office of the company represented by the visitor
   – personal identification type and number
   – purpose of visit

Data may only be recorded with the consent of the data subjects, the provision of the data implies consent to data processing. The register of the data of the sighted person is kept in paper form, and personal data recorded in the register are destroyed after 30 days.

4.1.4. Placing an anonymous visitor ID, analysing log files, sending special offers

Setting an anonymous visitor identifier (cookie)

An anonymous visitor identifier (cookie) is a unique set of signals that service providers place on visitors' computers to identify them and store profile information. It is important to note that such a sequence of signals, given that it does not store the full IP address, cannot in itself identify the customer, i.e. the visitor, in any way, but can only be used to recognise the visitor's computer. It is not necessary to provide a name, e-mail address or any other personal information, as the service provider does not ask the visitor for any data when using such solutions, the data exchange is in fact between machines.

In the networked world, personalised information and tailored service can only be provided if service providers can identify their customers' habits and needs. OFESZ, like other service providers, processes such anonymous identifiers, which no longer contain personal data as mentioned above, in order to learn more about customers' information usage patterns and thus improve the quality of its services, as well as to provide its customers with tailored pages and marketing (advertising) material when they visit its website.

If a visitor to the OFESZ website does not wish to have such an identifier placed on his/her computer, he/she can configure his/her browser to prevent the placing of the unique identifier. In this case, the data subject will still be able to use most of the OFESZ's services, but in some cases (for example, on OFESZ's pages offering customised solutions) OFESZ will not be able to serve the data subject to the fullest extent.

4.1.5. Analysis of log files

The analysis of log files generated by the use of web services provides useful information for service providers in several ways. In the log files, the servers providing the service record information about the requests sent by visitors, such as the dynamic IP address of the computer sending the request, the type of browser used, the time of the request, the address of the page requested, etc. Such information is used by OFESZ to analyse

the secure operation of its servers, for post-processing purposes, to maintain the security and availability of the website operated by OFESZ. The series of data thus obtained may also be combined with personally identifiable information from other sources by the OFESZ, where necessary for the smooth operation of the website and the evaluation of the data, or for the performance of the service provided by the Data Controller, or for quality assurance or market research purposes.

4.1.6. Sending special offers

OFESZ sends to its customers, subject to their consent, periodic information circulars about new services, special offers, etc. If our customers no longer wish to receive such promotional mailings, although they have not previously indicated their intention to do so, they may cancel them at any time in the same way and through the same channel as they used to request the service.

4.1.7. Research-Development project contribution

Your anonymised sample and data may be used in a research and development project for diagnostic and epidemiological purposes.

4.2. Transfer of personal data

Personal data processed by the OFESZ may be transferred in the following cases:

a. to the competent national security bodies, investigative authorities and the courts for the purposes of protecting national security, defence and public security, prosecuting public offences and the unauthorised use of the telecommunications system,
b. in the event of litigation, to the courts,
c. to contractors (accountants, lawyers, etc.) acting on behalf of the OFESZ in the course of its activities or administrative operation, to the extent necessary for the performance of their duties.

The recipients of data provided under subsection c) of this provision shall be bound by the same confidentiality obligations as the OFESZ.

4.2.1 Data processors:

Occupational health doctors
The doctors of the OFESZ's respective subcontractors with whom it has a contract of appointment. When carrying out an occupational health examination, they record the findings in the employee's health record or have access to the data that can be recorded here for the purposes of their duties under Act CLIV of 1997 and are therefore considered to be data processors.

The OFESZ uses Google Ads advertising software and Google conversion tracking, which use cookies to generate statistics (see below) and process traffic data, and Google is therefore a data processor (www.google.de/policies/privacy/).

Google Analytics
OFESZ uses Google Analytics primarily to produce statistics, including to measure the effectiveness of its activities. By using the program, OFESZ mainly obtains information on the number of visitors to its Website and the time spent on the Website. The programme

recognises the IP address of the visitor and can therefore track whether the visitor is a returning or new visitor, and can also track the path the visitor has taken on the Website and where they have accessed. The cookie has a lifetime of 14 months, after which time it is automatically deleted.

Google Remarketing
The OFESZ collects DoubleClick cookie data in addition to the usual Google Analytics data when using Google Remarketing. The DoubleClick cookie is used to use the remarketing service, which primarily ensures that visitors to the Website are subsequently exposed to OFESZ advertisements in free Google advertising spaces. OFESZ uses Google Remarketing for its online advertising. OFESZ's advertisements are also displayed on Internet sites by external service providers, such as Google. The Data Controller and third-party service providers, such as Google, use their own cookies (such as Google Analytics cookies) and third-party cookies (such as the DoubleClick cookie) together to track users' previous visits to the Website and to optimise and display advertisements.

Google Ads conversion tracking
The purpose of Google Ads conversion tracking is to enable OFESZ to measure the effectiveness of Ads advertising. This is done by means of cookies placed on the User's computer, which exist for 30 days and do not collect any personal data.

4.3. Data protection incident

In the event that the OFESZ becomes aware that a data breach has occurred, it shall notify the National Authority for Data Protection and Freedom of Information without undue delay and, where possible, within 72 hours of becoming aware of the incident, unless it considers that the data breach is unlikely to pose a risk to the rights and freedoms of data subjects.
The OFESZ will keep records of data breaches, indicating the facts relating to the data breach, its effects and the measures taken to remedy it.
Where a data breach is likely to result in a high risk to the rights and freedoms of data subjects, the OFESZ shall also inform data subjects of the data breach without undue delay.
In the event of a data breach in connection with the processing of data by the OFESZ, a notification can be made to the Data Protection Officer at the following e-mail address: kiraly.lilla@ofesz.hu

4.4. Rights of data subjects and their enforcement

4.4.1. Right of access:

The data subject has the right to receive feedback from the OFESZ on whether his or her personal data are being processed and, if such processing is taking place, the right to access the personal data and the following information:

the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipients to whom or with which the personal data have been or will be disclosed, including in particular recipients in third countries or international organisations (if any); the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period.

The data subject may request the rectification, erasure or restriction of the processing of his or her personal data, except for processing required by law, or object to the processing of

such personal data.

At the request of the data subject, the OFESZ as controller shall provide information about the data of the data subject processed by it or by a processor to whom it or it has delegated the processing, the source of the data, the purposes, legal basis and duration of the processing, the name and address of the processor and the activities of the processor in relation to the processing, and, in the case of a transfer of personal data of the data subject, the legal basis and the recipient of the transfer.

4.4.2. Right to rectification:

The data subject shall have the right to obtain, at his or her request and without undue delay, the rectification of inaccurate personal data relating to him or her. Having regard to the purposes of the processing, the data subject shall have the right to obtain the rectification of incomplete personal data, including by means of a supplementary declaration.

4.4.3. The right to erasure (forgetting):

The data subject has the right to have personal data relating to him or her erased by the OFESZ without undue delay upon his or her request, and the OFESZ is obliged to erase personal data relating to him or her without undue delay if one of the following grounds applies:

a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
b) the data subject withdraws his or her consent and there is no other legal basis for the processing;
c) the data subject objects to the processing and there is no overriding legitimate ground for the processing;
d) the processing of personal data is unlawful;
e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the OFESZ is subject.

The OFESZ will notify the data subject of the rectification and erasure, as well as all those to whom the data were previously disclosed for processing. The notification may be omitted if this is not prejudicial to the legitimate interests of the data subject in relation to the purposes of the processing.
If the OFESZ does not comply with the data subject's request for rectification, blocking or erasure, it shall, within 30 days of receipt of the request, communicate in writing the factual and legal grounds for refusing the request for rectification, blocking or erasure. If the request for rectification, erasure or blocking is refused, the OFESZ shall inform the data subject of the possibility of judicial remedy and of recourse to the Authority.

4.4.4. Right to restriction of processing:

Az érintett jogosult arra, hogy kérésére az OFESZ korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the OFESZ to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the data and requests instead the restriction of their use;
(c) the OFESZ no longer needs the personal data for the purposes of the processing, but

the data subject requires them for the establishment, exercise or defence of legal claims; or

(d) the data subject has objected to the processing; in this case, the restriction shall apply for a period of time until it is established whether the legitimate grounds of the OFESZ prevail over the legitimate grounds of the data subject.

4.4.5. Right to data portability:

The data subject has the right to receive personal data relating to him or her which he or she has provided to the OFESZ in a structured, commonly used, machine-readable format, and the right to transmit such data to another controller without the OFESZ preventing it, provided that:

(a) the processing is based on explicit consent or on a contract relating to the processing of special categories of personal data; and

(b) the processing is carried out by automated means.

On the basis of the right to data portability, the data subject also has the right to request, where technically feasible, the direct transfer of personal data between controllers.

The controller shall refuse to comply with the request where the data portability is restricted by law or where the exercise of the right to data portability by the data subject would adversely affect the rights and freedoms of others. The refusal shall be notified to the data subject within one month of receipt of the request.

The controller may not require any consideration for the provision of personal data unless the request is manifestly unfounded or excessive, in particular because of its repetitive nature.

The controller shall not be responsible for the processing of personal data by the data subject or by another company receiving the personal data.

4.4.6. Right to object:

The data subject may object to the processing of his or her personal data if.

- the processing (transfer) of personal data is necessary solely for the purposes of the exercise of a right or legitimate interest pursued by the OFESZ or the recipient, except in cases of mandatory processing;
- the personal data are used or further processed for direct marketing, public opinion polling or scientific research purposes, including profiling, where it is related to direct marketing; or
- the exercise of the right to object is otherwise permitted by law.

If the objection is justified, the OFESZ will terminate the processing, including further collection and transfer, and block the data, and notify the objection and any action taken in response to it to all those to whom the personal data concerned by the objection have been disclosed and who are obliged to take action to enforce the right to object.

4.4.7. Transparent information, communication and measures for the exercise of data subjects' rights

The OFESZ will inform you in writing (including by e-mail), without undue delay and in any event within one month of the request, of the action taken on the request (see points 4.4.1 to 4.4.6). If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The OFESZ will inform the person concerned of the extension, stating the reasons for the delay, within one month of

receipt of the request. If the data subject has submitted the application by electronic means, the OFESZ shall provide the information by electronic means, unless the data subject requests otherwise.

The information and action provided for in this point shall be provided by the OFESZ free of charge. If the request of the data subject is manifestly unfounded or excessive, in particular because of its repetitive nature, the OFESZ shall be subject to the administrative costs of providing the information or information requested or of taking the requested action:

- charge a reasonable fee; or
- refuse to act on the request.

If the re-information shows that the processing was unlawful or incorrect, the administrative fee will be refunded.
The OFESZ will examine the objection within the shortest possible period of time from the date of the request, but not exceeding 15 days, and will inform the applicant in writing of the outcome of the examination, with a simultaneous suspension of the processing of the data concerned by the objection. If the data subject disagrees with the decision taken by the OFESZ, he or she shall have the right to bring an action before a court within 30 days of the date of notification.

The data subject acknowledges that the OFESZ will not delete the data and is entitled to process the data for as long as the OFESZ has a claim against the data subject in connection with its business activities, whether in litigation or not. If no action is brought or if the data subjects have fulfilled their payment obligations to OFESZ arising from the business relationship, the data may be deleted after the limitation period.

Right to lodge a complaint with a supervisory authority
Without prejudice to other administrative or judicial remedies, all data subjects have the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information:

Name: National Authority for Data Protection and Freedom of Information
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410

4.5. Data security requirements

The OFESZ shall ensure the security of the data, take all technical and organisational measures and establish all procedural rules necessary to enforce the Regulation and other data protection and confidentiality rules. The OFESZ shall protect the data against unauthorised access, alteration, disclosure or deletion, damage or destruction. The OFESZ also undertakes to draw the attention of any third parties to whom it may transfer or disclose the data to the fulfilment of its obligations in this respect.

The personal data processed by the OFESZ shall comply with the following requirements:

- their collection and processing are fair and lawful,
- accurate, complete and timely,
- They are lawful, fair, complete, accurate, timely, complete, complete and proportionate, and stored in a manner which permits identification of data subjects for

no longer than is necessary for the purposes for which the data are processed and stored.

4.6. Data storage

Given that the OFESZ also maintains medical records (employees' medical records), it undertakes to keep employees' medical records for at least 30 years, except for imaging diagnostic images and findings, for at least 30 years from the date of recording, and the final report for at least 50 years.
The OFESZ may, where justified, continue to keep the stored data for the purposes of medical treatment or scientific research after the above-mentioned mandatory retention period. If further record-keeping is not justified and the medical records are of no scientific value, the OFESZ will destroy the records.
The OFESZ undertakes to keep the diagnostic imaging record for 10 years from the date of its production and the diagnostic report for 30 years from the date of its production.
In the event of the dissolution of the OFESZ without legal succession:
a) the medical documentation of scientific interest to the Semmelweis Museum, Library and Archives of Medical History,
b) other medical documentation shall be transferred to the body designated by the Government.

If the OFESZ is dissolved without legal succession, but the tasks previously performed by it are carried out by another body,
(a) the medical records generated in the 10 years preceding the date of the dissolution of the body which has been responsible for the documentation,
b) the medical records not transferred under point a) shall be transferred to the body designated by the Government.
For the purposes of data preservation, the OFESZ shall ensure at all times that the medium remains readable or is restored to a readable state under the technical conditions.
Otherwise, data retention shall be governed by the provisions of the law in force.

4.7. Data Protection Officer

The OFESZ appoints a Data Protection Officer to ensure that the requirements of data protection and data security are met in terms of staff and facilities. The Data Protection Officer shall be directly supervised by the Chief Executive.

The controller shall ensure that the DPO is involved in all matters relating to the protection of personal data in an appropriate and timely manner.
The DPO shall not accept instructions from any person in the performance of his or her duties. The DPO shall be directly responsible to the top management of the controller or processor.
The DPO shall be bound by an obligation of confidentiality or data protection in the performance of his or her duties.

The DPO shall provide information and professional advice to the controller or processor and to the employees carrying out the processing, monitor compliance with the controller's or processor's internal rules on the protection of personal data, provide professional advice on data protection impact assessment upon request, cooperate with the supervisory authority.

The OFESZ Data Protection Officer is the person appointed to carry out the duties of Data Protection Officer:

name: Gyöngyösiné Király Lilla Klára
contact details: kiraly.lilla@ofesz.hu; +36-20-779-2828

Tasks of the Data Protection Officer

- contributes to or assists with decisions relating to data management and the rights of data subjects;
- monitor compliance with the provisions of the Regulation and other OFESZ legislation on data processing, as well as with internal data protection and data security policies and data security requirements;
- provide technical advice on data protection impact assessments;
- investigate the notifications received and, where unauthorised processing is detected, require the controller or processor to cease such processing;
- cooperate with the Supervisory Authority (NAIH)
- draw up an internal data protection and data security policy;
- maintain internal data protection records;
- ensure data protection education.

8./ Destruction of files

The destruction of paper documents is mainly carried out in a shredder, under the supervision of the employee responsible for archiving.

Laws on which the processing is based

- REGULATION (EU) No 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 Regulation (EC) No 95/46/EC (General Data Protection Regulation)
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.
- Act LXVI of 1995 on public records, public archives and the protection of private archival material.
- Act CVIII of 2001 on certain aspects of electronic commerce services and information society services.
- Act V of 2013 on the Civil Code,
- Act XLVII of 1997 on the processing and protection of health data and related personal data,
- Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation (hereinafter referred to as the "Act on the Protection of Personal Data and the Protection of Property"),
- Act I of 2012 on the Labour Code (hereinafter: Labour Code Act I of 2012),
- the Fundamental Law of Hungary.