

L33 Kids Limited Liability Company

L33 KIDS SERVICE PROVIDER LIMITED LIABILITY COMPANY

# PRIVACY POLICY

## REGARDING THE PROCESSING OF PERSONAL DATA IN CONNECTION WITH HEALTHCARE SERVICES

Effective from 1 January 2025

I.	Objective of the Privacy Policy .....	4
II.	Controller's data.....	4
III.	Data processing activities .....	5
	(1) Data processing related to contact and appointment scheduling.....	5
	(2) Patient intake 1: recording the patient's personal data .....	6
	(3) Patient intake 2: Processing the personal data of the patient's legal representative. ....	7
	(4) Patient intake 3: the processing of contact details of the patient and the patient's legal representative.....	8
	(5) Keeping medical records.....	8
	(6) Records related to data protection submissions .....	9
	(7) Records of access to medical records, requests for access, requests for copies.....	10
	(8) Data processing related to invoicing .....	11
	(9) Data processing and registration of complaints .....	12
	(10) Records of access to data for scientific research purposes .....	13
	(11) Maintaining a record of data transfers .....	13
	(12) Reporting side effects to the pharmaceutical administrative authority.....	14
	(13) Reporting data to EESZT.....	15
	(14) Sending newsletters .....	16
IV.	Information on data processing .....	16
	(1) General information relating to processing based on the legitimate interests of the Controller: 16	
	(2) Recipients of personal data: .....	16
	(3) Method of data processing .....	17
	(4) General description of technical and organisational measures: .....	17
	(5) Measures taken to ensure data security.....	17
	(6) Creating backups.....	18
V.	Rights of the data subject in relation to data processing .....	18
	(1) How can the data subject exercise their rights? .....	18
	(2) Right of access .....	19
	(3) Right to rectification .....	19
	(4) Right to erasure .....	19
	(5) Right to restriction of processing .....	20
	(6) Right to object.....	20
	(7) Right to data portability .....	21

(8) Right to withdraw consent .....	21
(9) Right of disposition in the event of death .....	21
(10) Right to make a complaint.....	22
(11) Initiation of legal proceedings .....	22
VI. Closing Provisions.....	22
Annex 1 .....	23
Data processors and transfers used by the Data Controller .....	23

## I. Objective of the Privacy Policy

This Privacy Policy (hereinafter referred to as the "**Policy**") summarises the processing of personal data by L33 Kids Service Provider Limited Liability Company as the data controller (hereinafter referred to as the "**Controller**") in relation to healthcare.

In this Privacy Policy, we wish to inform the individuals who use the healthcare services of the Data Controller, as well as those who make appointments for the provision of healthcare services, their legal and authorised representatives, relatives and other persons involved in the healthcare process (hereinafter referred to as "Data Subjects"), about the details of the processing of their personal data in the context of the healthcare activities of the Data Controller, in compliance with the provisions of the Regulation 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 of the European Parliament and of the Council of 2016 (hereinafter referred to as "GDPR").

With this Privacy Policy, **L33 Medical Ltd.** primarily aims to comply with:

- Article 12 of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter referred to as GDPR), applicable from 25 May 2018,
- Article 20 of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter referred to as Infotv.),
- Act XLVII of 1997 on the management and protection of health and related personal data (hereinafter referred to as Eüak.), and
- Decree 62/1997 (XII.21) NM on certain issues of the management of health and related personal data.

The company takes measures to ensure that all essential information and explanations are presented to natural persons affected by the handling of health and identification data in a concise, transparent, understandable, and easily accessible form, clearly and comprehensibly worded, and to assist them in exercising their rights.

## II. Controller's data








Name:	L33 Kids Service Provider Ltd.
Registered seat:	2040 Budaörs, Lévai u. 33.
Represented by:	Adrienn Benkő, Dr. managing director
Company registration number:	Cg. 13-09-225319
Tax number:	32199549
Phone number:	+36 23 200 217
E-mail address:	kids@l33medical.hu
Website:	<a href="https://kids.l33.hu/">https://kids.l33.hu/</a>
Data Protection Officer:	dpo.kids@l33.hu

### III. Data processing activities

#### (1) Data processing related to contact and appointment scheduling

**Description of the activity:** Appointments can be scheduled in person, by telephone, or via the contact form available on the Data Controller's website. When scheduling an appointment, the patient provides certain contact information along with other details necessary for the appointment (e.g. the service they wish to receive). The Data Controller manages and records appointments on paper, including the personal data necessary for scheduling the appointment of the concerned patient.

	<b>Data subjects:</b>	who wishes to benefit from the healthcare services provided by the Data Controller	
	<b>Purpose of processing:</b>	providing appointments and organizing services for patients arriving for healthcare purposes.	
		using email and phone numbers for maintaining contact with patients within the scope of service organization (e.g., sending reminders about appointments).	
	<b>Legal basis for processing:</b>	identification of the patient	
		processing is necessary for the purposes of taking steps at the request of the data subject prior to entering into a contract; [Article 6(1)(b), 2nd indent, of the GDPR].	
	<b>Scope of the data processed and purpose of data processing:</b>	<b>Scope of the data processed</b>	<b>Purpose of processing</b>
		name of the patient, name of the contact person	identification of the patient
		patient's telephone number, e-mail address	keeping in touch, sending a reminder text message about the appointment
		type of service to be used	preparation of the examination, referral to a specialist with the appropriate qualifications
	<b>Duration of storage of personal data:</b>	6 months from the date of data collection	
	<b>Consequences of failing to provide the data:</b>	no appointment can be scheduled; no healthcare services can be utilized.	
	<b>How the data comes to the attention of the controller:</b>	the person scheduling the appointment, who may be the patient or another person acting on the patient's behalf (e.g. relative, legal representative)	



<b>Special data category:</b>	data relating to health status
<b>Additional conditions for the processing of special categories of data:</b>	the provision of healthcare or treatment [Article 9(2)(h) GDPR].

## (2) Patient intake 1: recording the patient's personal data

**Description of the activity:** The registration and identification of the patient is carried out in the form regulated by the Controller. The patient must prove their identity with an identification document and present their social security card as well as their address card. At the time of intake, the personal data necessary for the patient's care are recorded in the electronic information system of the Controller. At the time of intake, the patient provides personal data in writing on the form provided by the Controller (anamnesis form). In certain cases, the patient provides written consent for the examination or procedure to be carried out.



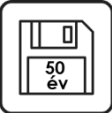


<b>Data subjects:</b>	the person receiving the health care service
<b>Purpose of processing:</b>	promoting the preservation, improvement and maintenance of health
	facilitating the effective medical treatment activities of the healthcare provider.
	monitoring the health status of the individual concerned
	providing the necessary consent to the medical procedure



<b>Legal basis for processing:</b>	fulfilment of the Data Controller's legal obligations [Article 6 (1) (c) GDPR, Articles 136 and 3 (p) of the Eütv; Articles 15 (2) - (3) and (4) - (5) of the Eütv]. The processing is not voluntary and is independent of the data subject's will.
------------------------------------	---






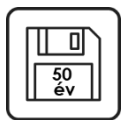

<b>Scope of the data processed and purpose of data processing:</b>	<b>Scope of the data processed</b>	<b>Purpose of processing</b>
	the patient's name, name at birth, mother's name at birth, place of residence, place and date of birth, address, passport number for foreigner individuals and the name of their legal representative	identification of the patient and their legal representative, recording this information in the medical documentation
	the patient's social security number	identification of the patient in the healthcare system, fulfilment of the obligation to transmit data to the EESZT

		the medical data provided in the consent statement for the examination or medical procedure	reducing the risks associated with the examination or the medical procedure, assessing its feasibility from a medical professional's perspective, and performing the examination or procedure.
	<b>Duration of storage of personal data:</b>	30 years from the date of data collection, and 50 years for the discharge summary (Article 30 of the Eüak).	
	<b>Consequences of failing to provide the data:</b>	Healthcare services cannot be provided to the patient.	
	<b>How the data comes to the attention of the controller:</b>	it is provided by the patient or their representative.	
	<b>Special data category:</b>	data on health status	
	<b>Additional conditions for the processing of special categories of data:</b>	establishment of a medical diagnosis, the provision of healthcare or treatment [Article 9(2)(h) GDPR].	

### (3) Patient intake 2: Processing the personal data of the patient's legal representative.





**Description of the activity:** In certain cases, the patient's legal representative is entitled to provide consent to a medical procedure or examination on behalf of the patient. The legal representative must provide credible proof of identity and status. The Controller shall retain the original copy of the authorisation. The personal identification data of the legal representative is recorded in the patient's medical documentation.

	<b>Data subjects:</b>	the patient's legal representative.
	<b>Purpose of processing:</b>	verification and documentation of the identity of the legal representative and the title of the representation, as well as ensuring its subsequent provability.  providing consent to a medical procedure or examination on behalf of the patient
	<b>Legal basis for processing:</b>	fulfilment of a legal obligation of the Controller [Article 6(1)(c) GDPR, and Articles 136 and 3(p) of the Eütv. The processing is not voluntary and is independent of the data subject's will.
	<b>Scope of the data processed</b>	the personal identification data of the legal representative
		the title of the representation and other personal data contained in the document verifying it

 	<b>Duration of storage of personal data:</b>	30 years from the date of data collection, and 50 years for the discharge summary (Article 30 of the Eüak).
	<b>Consequences of failing to provide the data:</b>	The medical procedure or examination cannot be carried out.
	<b>How the data comes to the attention of the controller:</b>	it is provided by the legal representative

(4) **Patient intake 3: the processing of contact details of the patient and the patient's legal representative**

**Description of the activity:** The telephone number and/or e-mail address and residential address of the patient and the patient's legal representative will be registered in the patient's medical record at the time of the patient intake. The reason for this is to ensure that the patient can be contacted in case of any subsequent events that may affect the examination, treatment, or the patient's health condition. In addition, the Controller sends appointment reminder notifications related to the patient's treatment via email or text to the patient or their legal representative.






	<b>Data subjects:</b>	the patient the patient's legal representative.
	<b>Purpose of processing:</b>	Communication with the patient and their legal representative. Sending reminder messages about appointments.
	<b>Legal basis for processing:</b>	consent of the data subject, [Article 6(1)(a) GDPR].
	<b>Scope of the data processed:</b>	the telephone number, e-mail address and place of residence of the patient and/or the patient's legal representative
	<b>Duration of storage of personal data:</b>	until consent is withdrawn or for 10 years after the last contact
	<b>Consequences of failing to provide the data:</b>	communication with the patient and their legal representative cannot be established
	<b>How the data comes to the attention of the controller:</b>	it is provided by the patient or the legal representative.

(5) **Keeping medical records**

**Description of activity:** the Data Controller retains medical documentation generated in the course of providing its services in both electronic and paper formats.



<b>Data subjects:</b>	the individual receiving the healthcare service and their legal representative.
-----------------------	---





	<b>Purpose of processing:</b>	compliance with medical documentation requirements
	<b>Legal basis for processing:</b>	fulfilment of a legal obligation of the Controller [GDPR Article 6(1)(c) and Article 136 of the Eütv]. The processing is not voluntary and is independent of the data subject's will.
	<b>Scope of the data processed:</b>	personal identity and health data registered in the medical documentation.
	<b>Duration of storage of personal data:</b>	medical documentation must be retained for 30 years from the date of data collection, imaging diagnostic recordings for 10 years from the date of their creation, medical findings derived from such recordings for 30 years from the date of the recording, and discharge summaries for 50 years. (Article 30 (1)-(2) of the Eüak).
	<b>Special data category:</b>	data on health status
	<b>Additional conditions for the processing of special categories of data:</b>	establishment of a medical diagnosis, the provision of healthcare or treatment [Article 9(2)(h) GDPR].

#### (6) Records related to data protection submissions



**Description of the activity:** Under the GDPR, data subjects have certain rights in relation to the processing of their personal data. These rights are described in detail in Section III.6 of this Policy. The Controller shall keep a record of the exercise of these rights and of the measures taken in connection therewith and shall keep the documents generated in connection with the exercise of the rights.



	<b>Data subjects:</b>	the patient, the patient's legal representative or authorised representative
	<b>Purpose of processing:</b>	<p>keeping records of the exercise of the rights of the data subject in relation to the processing of their personal data and preserving documentation associated with the exercise of these rights.</p> <p>recording the frequency with which the data subject exercises their rights.</p> <p>ensuring the principle of accountability under the GDPR</p>
	<b>Legal basis for processing:</b>	the legitimate interest of the Controller [Article 6(1)(f) GDPR]. It is in the legitimate interest of the Data Controller to be able to verify when and what action it has taken in relation to the data subject's requests and thereby complied with the provisions of the GDPR. The Data Controller can verify compliance by keeping separate records in view of the potentially large number of requests.

	<b>Scope of the data processed:</b>	the content of the data subject's request
		contents of the records on the exercise of data subject rights (the name of the individual enforcing the right, the name of the data subject, the method and date of receipt of the request, the subject of the request, the date and method of any action taken to restrict or deny the exercise of the data subject's right, along with the legal and factual reasons for it, confirmation of the fulfilment of the data subject's right, and the date on which the data subject's request was fulfilled).
		copies of documents proving the applicant's exercise of their rights,
		identity details of the applicant
	<b>Duration of storage of personal data:</b>	until the expiry of the retention period of the personal data concerned by the exercise of the right.
	<b>Consequences of failing to provide the data:</b>	the request cannot be granted.
	<b>How the data comes to the attention of the controller:</b>	shall be provided by the applicant.

#### (7) Records of access to medical records, requests for access, requests for copies




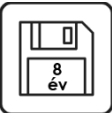

**Description of the activity:** In certain cases, legislation authorizes individuals other than the patient to access healthcare data, review medical documentation, and request copies of such documentation. The Data Controller shall keep a record of such requests and of the action taken in response to them, and shall keep copies of the documents supporting the lawfulness of the exercise of the right. The Controller shall verify the identity and the right of the applicant to request a copy and requests documents proving the conditions for the right to request copies as defined by law. If the patient exercises these rights, the Controller shall record this in the register of data protection submissions (see Section (6)).

	Data subjects:	the patient and their legal or authorised representative
		any other person entitled by law to obtain copies, access, or information.
	Purpose of processing:	the verification and ex post verifiability of the lawfulness of the exercise of rights,
		ensuring the principle of accountability under the GDPR
	Legal basis for processing:	the legitimate interest of the Controller [Article 6(1)(f) GDPR]. It is in the Controller's legitimate interest to verify to whom, when and on what legal basis it has granted access to the patient's personal data and medical records and that its actions have been lawful.

	<b>Scope of the data processed:</b>	copies of documents proving the applicant's right of access
		the substantive elements of the application
		identity details of the applicant
		personal data in the patient's medical records
		the contents of the exercise of the right (name of the person exercising the right, name of the patient, manner and date of receipt of the request, subject of the request, date, manner and legal and factual grounds for taking the measure restricting or refusing to exercise the right, fact of the applicant's right, date of execution of the request)
	<b>Duration of storage of personal data:</b>	five years from the fulfilment or rejection of the exercise of rights (limitation period).
	<b>Consequences of failing to provide the data:</b>	it is not relevant, as the data is generated by the Controller.

#### (8) Data processing related to invoicing

**Description of the activity:** the Controller issues an invoice to the patient or other person (e.g. in cases where a fee is applied for issuing a copy). The invoice shall include the personal details of the patient or other person and the service received.

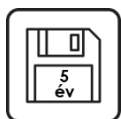
	<b>Data subjects:</b>	to whom the invoice is issued
	<b>Purpose of processing:</b>	fulfilment of invoicing and storage obligations
	<b>Legal basis for processing:</b>	fulfilment of the Controller's legal obligations [Article 6 (1) (c) GDPR, Article 159 (1) and 169 (e) to (f) of Act CXXVII of 2007 on Value Added Tax, Articles 166 (1)-(3), 167 and 169 (2) of Act C of 2000 on Accounting (hereinafter: <b>Sztv.</b> )]. The processing is not voluntary and is independent of the data subject's will.
	<b>Scope of the data processed:</b>	The invoice includes the name and address of the recipient, the name of the health service used, the date of issue.
	<b>Duration of storage of personal data:</b>	8 years from the date of issue of the invoice (Article 169 (2) of the Sztv.).
	<b>Consequences of failing to provide the data:</b>	no invoice can be issued, the service cannot be provided.



<b>How the data comes to the attention of the controller:</b>	is provided by the service user.
<b>Special data category:</b>	data on health status
<b>Additional conditions for the processing of special categories of data:</b>	provision of healthcare or treatment [Article 9(2)(h) GDPR].

## (9) Data processing and registration of complaints

**Description of the activity:** the patient has the right to file a complaint with the Controller about the medical treatment. The Controller shall investigate the complaint and inform the patient of the outcome in writing as soon as possible, but not later than 30 working days. Complaints must be recorded and the documents relating to the complaint and its investigation must be kept for 5 years. The patient is entitled to act through a Patient Rights Advocate or another authorized representative.



<b>Data subjects:</b>	a complainant
	the patient
	the representative of the complainant or patient
	Patient Rights Advocate
<b>Purpose of processing:</b>	fulfilling the legal obligation to investigate and record patient complaints and to preserve documentation related to these complaints.
<b>Legal basis for processing:</b>	fulfilment of the Controller's legal obligation [Article 6 (1) (c) GDPR, Article 29 (4) of Act CLIV of 1997 (Eütv.)]. The processing is not voluntary and is independent of the data subject's will.
<b>Scope of the data processed:</b>	the data contained in the complaint and the response to it
	data generated during the investigation of the complaint
	the data included in the complaint management register (name of the complainant, date of the complaint, method of communication of the complaint, date of receipt of the complaint, summary of the content of the complaint, date of reply to the complaint, summary of the content of the reply, method of reply to the complaint, name of the health centre concerned by the complaint).
<b>Duration of storage of personal data:</b>	5 years from the date of the reply to the complaint (Article 29 (4) of the Eütv).
<b>Consequences of failing to provide the data:</b>	the complaint cannot be investigated.
<b>How the data comes to the attention of the controller:</b>	is partly provided by the complainant and partly arises during the investigation of the complaint.
<b>Special data category:</b>	data on health status



**Additional conditions for the processing of special categories of data:**

provision of healthcare or treatment [Article 9(2)(h) GDPR].

#### (10) Records of access to data for scientific research purposes

**Description of the activity:** For the purposes of scientific research, the stored data may be accessed with the joint approval of the Controller's Chief Executive Officer, the professional leader and the Data Protection Officer. However, no health and personal data may be included in a scientific communication in a manner that would allow the identification of the data subject. Copies of the stored data that include personally identifiable information cannot be made. A record must be kept of the individuals who accessed the stored data, the purpose of the access and the time of access. The record must be kept for 10 years.



**Data subjects:**

the patient, the person requesting access to data for scientific research

**Purpose of processing:**

fulfil the obligation to keep records of access for scientific research purposes.



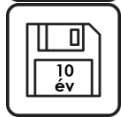
**Legal basis for processing:**

fulfilment of the Controller's legal obligations [Article 6 (1) (c) GDPR, Article 21 (2) of Act XLVII of 1997 (Eüak.)]. The processing is not voluntary and is independent of the data subject's will.



**Scope of the data processed:**

data recorded about individuals who access information for scientific research purposes



**Duration of storage of personal data:**

10 years from the date of access (Article 21 (2), Eüak.).

**Consequences of failing to provide the data:**

it is not relevant, as the data is generated by the Controller.

**How the data comes to the attention of the controller:**

is available at the Controller.

#### (11) Maintaining a record of data transfers

**Description of the activity:** The Controller is required by law to transfer to a third party the medical and personal identification data collected from a patient for the purposes of medical treatment. The Controller examines the lawfulness of such requests in accordance with the procedures set out in the Privacy Policy and, if the request complies with legal requirements, it shall be fulfilled. The Controller shall keep a record of such requests, along with the actions taken to address them.



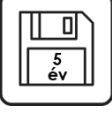


**Data subjects:**

the individual using health services




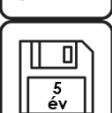


**Purpose of processing:**

fulfilling the obligation to keep records of data transmission

	<b>Legal basis for processing:</b>	fulfilment of the Controller's legal obligations [Article 6(1)(c) GDPR, Article 28(1) of Eüak.] The processing is not voluntary and is independent of the data subject's will.
	<b>Scope of the data processed:</b>	the patient's forwarded medical and personal identification data
	<b>Duration of storage of personal data:</b>	5 years from the transfer (limitation period).
	<b>Consequences of failing to provide the data:</b>	is not relevant, the data is available at the Controller.
	<b>How the data comes to the attention of the controller:</b>	is available at the Controller.





(12) Reporting side effects to the pharmaceutical administrative authority.

**Description of the activity:** A healthcare worker must report any suspected side effect that they observe or become aware of to the pharmaceutical administrative authority without delay. The notification must be made by filling in the form provided by the pharmaceutical administrative authority.

	<b>Data subjects:</b>	the patient
	<b>Purpose of processing:</b>	fulfilling the legal obligation to notify
	<b>Legal basis for processing:</b>	fulfilment of the Controller's legal obligations [Article 6(1)(c) GDPR, Article 18(2) of the Medicines Act]. The processing is not voluntary and is independent of the data subject's will.
	<b>Scope of the data processed:</b>	the content of the side effect report form provided by the pharmaceutical administrative authority
	<b>Duration of storage of personal data:</b>	5 years after the side effect was reported (limitation period)
	<b>Consequences of failing to provide the data:</b>	is generated at the Controller in the course of the investigation
	<b>How the data comes to the attention of the controller:</b>	Is available at the Controller.
	<b>Addressee:</b>	pharmaceutical administrative authority, which on the date of entry into force of this Policy is the National Public Health and Pharmaceutical Centre (1097 Budapest, Albert Flórián út 2-6. Email: info@egeszsegvonat.gov.hu)
	<b>Frequency of data transmission:</b>	occasional

### (13) Reporting data to EESZT

**Description of the activity:** The Controller shall comply with the obligation to transfer data to the Electronic Health Service Space (EESZT). In this context, the Controller shall transmit the personal data of the patients to the EESZT, as defined by law.

  	<b>Data subjects:</b>	the person to whom the Data Controller provides a healthcare service
	<b>Purpose of processing:</b>	Fulfilling the mandatory data provision requirements for the operation of the EESZT system
	<b>Legal basis for processing:</b>	fulfilment of the Controller's legal obligations [Article 6(1)(c) GDPR, Articles 35/F, 35/K of the Eüak; Articles 6, 12, 19, 20/A of EMMI Decree 39/2016 (XII.21.). The processing is not voluntary and is independent of the Data Subject's will.
	<b>Scope of the data processed:</b>	<ul style="list-style-type: none"> <li>- the social security number of the Data Subject or, in the absence of such number, another identifier, date of birth, gender, nationality in the case of prescriptions and referrals transmitted via the EESZT system, other personal identification data included in the prescription and referral, as well as the individual's identifier generated within the EESZT system,</li> <li>- the designation, type, date and duration of the care event and other data and documents specified in a ministerial decree,</li> <li>- the health care provider providing the care event, the EESZT identifier and the EESZT identifier of the person providing or contributing to the care,</li> <li>- the personal data contained in the finding,</li> <li>- Data to be provided to the EESZT central event catalogue according to Annex 1 of EMMI Decree No. 39/2016 (XII.21.) EMMI.</li> </ul>
	<b>Consequences of failing to provide the data:</b>	Not applicable, as the data is generated by the Controller during the examination or treatment
	<b>How the data comes to the attention of the controller:</b>	It is provided by the patient or their representative and is generated by the Controller in the course of providing healthcare services.
	<b>Addressee:</b>	National Hospital Directorate-General <a href="https://okfo.gov.hu/">(https://okfo.gov.hu/</a> , <a href="mailto:helpdesk.eeszt@okfo.gov.hu">helpdesk.eeszt@okfo.gov.hu</a> , address: <u>1125 Budapest, Diós árok 3.</u> Phone: (+361) 356-1522), contact details for the privacy policy: <a href="https://e-egeszsegugy.gov.hu/documents/26398/557047/EESZT_L">https://e-egeszsegugy.gov.hu/documents/26398/557047/EESZT_L</a>



	<a href="#">akossagi adatkezelesi tajekoztato 2021 v6.pdf/8678cf08-dbec-407d-03a9-f8e34e22fa43</a>
Frequency of data transmission:	continuous
Special data category:	data on health status
Additional conditions for the processing of special categories of data:	provision of healthcare or treatment [Article 9(2)(h) GDPR].

#### (14) Sending newsletters

**Description of the activity:** The Controller informs subscribers by telephone and/or e-mail about its additional services, discounts and offers. The Controller sends a newsletter to subscribers.



Data subjects:	who subscribes to the newsletter
Purpose of processing:	notifying subscribers about additional services, discounts and offers of the Controller.
Legal basis for processing:	the data subject's consent [Article 6(1)(a) GDPR].
Scope of the data processed:	e-mail address and/or telephone number
Duration of storage of personal data:	until the consent is withdrawn.
Consequences of failing to provide the data:	No newsletter can be sent.
How the data comes to the attention of the controller:	Provided by the data subject.

## IV. Information on data processing

#### (1) General information relating to processing based on the legitimate interests of the Controller:

Regarding data processing based on the legitimate interest of the Data Controller, the Data Controller has conducted the balancing test. On the basis of legitimate interest, the Controller shall not process personal data that would be incompatible with the purposes of the contract between the Controller and the patient.

#### (2) Recipients of personal data:



- employees, contractors of the Controller performing financial, tax, invoicing, controlling, auditing tasks, the Controller's managing director, employees performing administrative tasks, data processors of the Controller;



- court, police, other public authorities, and state agencies may, within the framework of their official proceedings, request the Data Controller on the basis of a legal authorisation to transmit personal data;
- National Tax and Customs Administration (<http://nav.gov.hu/>);
- a lawyer acting as legal representative;
- EESZT (Electronic Health Service Space), operated by the National Directorate General of Hospitals;
- The (personal) contributors of the Controller.
- Processors contracted by the Controller
- Annex 1 to this Policy sets out the data processors contracted by the Controller.

The Data Controller ensures that the recipients of personal data may only access such data strictly to fulfil their contractual obligations and only to the extent necessary for that purpose. They do not have general authorization to access all personal data.

### **(3) Method of data processing**

In paper format, stored in a cabinet lockable with a key or other secure means, and/or electronically.

### **(4) General description of technical and organisational measures:**

The organisational measures described in the Privacy Policy and in the management instructions on data protection.

### **(5) Measures taken to ensure data security**

Data backups and equivalent limited data retention and related data security activities are in the essential interests of the Controller to ensure business continuity and legal compliance. Since the primary goal of business continuity (and consequently data backup) and legal compliance is to ensure the triad of confidentiality, integrity, and availability — an objective pursued by minimizing risks that may jeopardize these principles — the specific details of related measures (such as timing, designation of specific subsystems, etc.) are not made public.

The Controller ensures the security of the Data Subjects' personal data by the following data security measures.

- The personal data are accessed by a specific group of persons within the organisation of the Controller only to the extent and for the purposes necessary for the performance of their work (see above, the list of recipients).
- The Controller has adopted a Privacy Policy, published it in a management directive and instructed its employees to read and comply with it.
- Provide data protection training as set out in the Privacy Policy.
- Data protection training consists of data protection law and information security.
- For the privacy training, educational materials are prepared, which will be sent to employees via email.

- Appointing a Data Protection Officer and their extensive involvement in making decisions related to data protection.
- Software and hardware-based information and communication security tools.
- Active and passive information security procedures supported by information communication and administrative tools.
- Monitoring processes implemented through separate subsystems.
- Regular (daily) backups of electronically stored data are created in such a way that, in the event of data damage — depending on the criticality of the data and the subsystem—the last undamaged state or the calendar day state defined by the backup plan can be restored. The Controller stores the backups on its own server or through its IT partner. Duration of backup storage: up to 1 year.

## **(6) Creating backups**

The purpose of creating backups is to enhance data security, comply with GDPR requirements, prevent incidents and events that may harm the interests of the Data Controller, mitigate the consequences of such events, ensure the availability and retrieval of official documents and communications, preserve certain work-related documents necessary for official operations and work processes, and restore them in case of data security issues to maintain workflow continuity.

The legal basis for the backup is the legitimate interest of the Controller [Article 6(1)(f) GDPR].

# **V. Rights of the data subject in relation to data processing**

## **(1) How can the data subject exercise their rights?**

The Data Subject may contact the Controller's representative directly with any requests, questions, complaints or comments regarding the Controller's conduct at the following contact details:

E-mail: [dpo.kids@l33.hu](mailto:dpo.kids@l33.hu)

The Data Subject may exercise their rights in relation to data processing by making a request to the Controller. The Controller shall respond to any request made using any of its contact details without undue delay and at the latest within 30 days.

Please contact us electronically if possible. Please be informed that the Controller will respond to data protection requests in electronic form wherever possible, unless the Data Subject explicitly requests another means of contact, or the Controller has no knowledge of the Data Subject's electronic contact details, or the Controller considers it necessary to verify the identity of the applicant for data protection reasons.

Please be informed that if the request for the release of the data entails disproportionate additional costs for the Controller (e.g. due to the format chosen), the Controller is entitled to charge the Data

Subject for the costs related to the release of the data. The Controller shall inform the Data Subject in advance of any costs incurred.

The Controller makes decisions regarding the evaluation of requests based on the legal grounds for data processing. You are entitled to exercise your above-mentioned rights as follows:

	Consent	Performance of the contract	Legal obligation	Legitimate interest
right of access	X	X	X	X
request for rectification	X	X	X	X
restriction	X	X	X	X
erasure	X	X		X
objection				X
data portability	X			
consent revocation	X			
right to complaint	X	X	X	X
right to judicial remedy	X	X	X	X

## **(2) Right of access**

On the basis of this right, the Data Subject may request to be informed about their personal data processed by the Controller and the circumstances surrounding the processing, in particular, but not limited to, the purposes for which their personal data are processed, the duration of the storage of the data, the recipients of the data in case of their transfer to third parties, and the details of automated decision making.

## **(3) Right to rectification**

If the Controller processes the Data Subject's personal data with inaccurate content, whether due to the Controller's fault or beyond its control, the Data Subject may request rectification of their data processed by the Controller under this right. If the purpose of the data processing allows it, the Data Subject may also request the completion of their incomplete data.

## **(4) Right to erasure**

The Data Subject may request the erasure of their personal data by the Controller if one of the following situations applies:

- processing of the personal data is no longer necessary for the purposes of the processing;
- where the processing was based on the Data Subject's consent and the data subject withdraws that consent, provided that there is no other legal basis for the processing of their personal data;
- the Data Subject objects to the processing of their personal data;
- the personal data have been unlawfully processed by the Controller;

- the Controller is required by law to delete personal data;
- the Data Subject's personal data were collected by the Controller in connection with an information society service before the Data Subject came of age.

We are unable to fulfil your request for the deletion of your personal data in the following cases:

- the processing of the data is necessary for the free expression of opinions or information of others;
- the Controller is required by law to process the data;
- the processing is necessary for a public health purpose;
- the processing is necessary for archival, scientific, historical research or statistical purposes;
- the processing is necessary for the establishment, exercise or defence of legal claims.

#### **(5) Right to restriction of processing**

The Data Subject may request the Controller to restrict the processing of their data if:

- the Data Subject contests the accuracy of the personal data, in this case, the restriction applies for the duration needed to clarify the accuracy of the data;
- personal data have not been lawfully processed by the Controller, but the Data Subject requests the restriction of processing instead of erasure;
- the Controller no longer needs the personal data for the purposes of processing, but the Data Subject explicitly requests their retention for the establishment, exercise or defence of a legal claim;
- the Data Subject objects to the processing of their personal data, in which case the restriction will apply for the period of time until we take a decision on their objection.

If we restrict the processing of your personal data based on your request, you will be informed in advance before the restriction is lifted. During the period of restriction, we will not process the Data Subject's personal data in any way other than storing them, unless one of the following applies:

- the Data Subject has consented to the processing of the data;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for an important public interest.

#### **(6) Right to object**

If the Controller processes personal data on the basis of its own legitimate interests or on the basis of the legitimate interests of another person, or if it processes personal data within the framework of performing a public task, the Data Subject may object to the processing at any time.

In the event of objection, we will stop processing your personal data, unless one of the following applies:

- there are compelling legitimate grounds for processing the data;
- processing for archival, scientific or historical research purposes, or statistical purposes is necessary for reasons of public interest.

## **(7) Right to data portability**

If personal data are processed automatically based on the Data Subject's consent or for the performance of a contract with the Data Subject, the Data Subject may request that the personal data provided by them to the Controller be transferred in a structured, commonly used, machine-readable format

- to the Data Subject, or
- enable its seamless transfer to another controller, or
- if the technical conditions are met, transfer it directly to the controller designated by the Data Subject.

However, we will not be able to comply with the request if any of the following applies:

- the processing is necessary for an important public interest;
- compliance with the request would adversely affect the rights of others.

## **(8) Right to withdraw consent**

If we process personal data on the basis of the Data Subject's consent, the Data Subject has the right to withdraw it at any time. In the event of withdrawal of consent, we will cease processing and delete your personal data, provided that there is no other legal basis for processing your personal data.

The withdrawal of consent shall not have any consequences for the Data Subject. However, the withdrawal of consent does not affect the lawfulness of our processing based on the consent given prior to that withdrawal.

The Data Subject may make a request concerning the above rights in writing or electronically, addressed to the Controller at the Controller's contact details set out in Section II:

The Controller shall decide on the request without undue delay, at the latest within one month of its receipt, and shall inform the Data Subject of the action taken on the request or, if no action is taken, of the reasons for the lack of action, and of the possibility of lodging a complaint with the supervisory authority or a judicial remedy.

The deadline for action may be extended by a further two months if necessary, taking into account the complexity of the application and the number of requests. The Controller shall inform the Data Subject of the extension of the time limit, stating the reasons for the extension, within one month of receipt of the request.

If the Data Subject's request is manifestly unfounded or excessive, the Controller may charge a fee or refuse to act on the request.

## **(9) Right of disposition in the event of death**

The Data Subject has the right to authorize a person at the Controller, either through a private document with full probative value or a public document. If the Data Subject has made several declarations at the Controller, the declaration made at a later date shall apply. This authorization allows the designated

person to exercise the rights granted to the Data Subject during their lifetime, within five years after their death.

- right to access (Section (2));
- right to rectification (3));
- right to erasure ((4));
- right to restriction of processing (Section (5));
- right to objection ((6));

#### **(10) Right to make a complaint**

The Data Protection Officer can be contacted with any questions, objections or complaints regarding data processing.

If you consider that the processing of your personal data does not comply with the applicable legal requirements, you may lodge a complaint with the data protection supervisory authority of any Member State of the European Union.

In Hungary, the data protection supervisory authority is the National Authority for Data Protection and Freedom of Information, whose contact details are:

Mailing address: 1363 Budapest, P.O. Box 9

Registered seat: 1125 Budapest, Falk Miksa utca 9-11.

Phone: +36 (1) 391-1400, +36 (30) 683-5969, +36 (30) 549-6838

Fax: +36 (1) 391-1410

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

Website: <http://naih.hu>

#### **(11) Initiation of legal proceedings**

The Data Subject may also enforce their rights in court. The court of law has jurisdiction to hear the case, and the Metropolitan Court of Budapest has jurisdiction to rule on the case. The lawsuit may also be brought before the court of the place of residence or domicile of the Data Subject (the contact details of the courts can be found at the following link: <http://birosag.hu/torvenyszekek>).

## **VI. Closing Provisions**

For matters not covered by this Privacy Poli, the provisions of Hungarian law on data protection, in particular the Infotv. and the GDPR applicable as of 25 May 2018, shall prevail. For further information, please contact any member of the Data Controller's staff or the Data Protection Officer.

This notice shall be effective from 1 January 2025 until its withdrawal, subject to review by the Data Controller every 3 (three) years at the latest.

Dated in Budaörs on the 21st day of November 2024.

**Annex 1**  
**Data processors and transfers used by the Data Controller**

<b>Name</b>	<b>Contact information</b>	<b>Activity</b>
NeedIT Services Ltd.	info@needit.hu	performing administrator activities
Cont-roll Pont Accounting Office	controllpont@gmail.com	accounting services
Digitalegg Ltd.	2045 Törökbálint, FSD park 4	hosting service
National Hospital Directorate-General	1125 Budapest, Diós árok 3. Fax: +36 (+361) 356-1522  <a href="https://okfo.gov.hu/helpdes">https://okfo.gov.hu/</a> <a href="mailto:k.eeszt@okfo.gov.hu">helpdes k.eeszt@okfo.gov.hu</a>	Operating EESZT; collecting healthcare-related information pertaining to a specific individual and make it accessible to authorized users through a secure electronic channel