Mediversal Egészségügyi Szolgáltató Kft.
registered office: 6725 Szeged, Semmelweis u. 8.
company registration number: 06-09-011070
tax number: 13882495-2-06

Privacy Policy

The Controller, Mediversal Egészségügyi Szolgáltató Kft. (registered office: 6725 Szeged, Semmelweis utca 8.; tax number: 13882495-2-06; company registration number: 06-09-011070; represented by: Viktor Vaszari, Managing Director; Data Protection Officer: Dr. Krisztián Bölcskei, available by post at the Controller's headquarters or electronically at adatvedelem@mediversal.hu) hereby complies with the requirements of Articles 13 and 14 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as: "GDPR") in relation to the processing of personal data and its obligation of compulsory disclosure.

In the interest of providing transparent information

- data processing is tabulated,
- a separate chapter contains a general description of the organisational and technical measures taken in relation to data security,
- details of your rights and how to exercise them are set out at the end of this privacy policy.

Description of data processing:	**Data processing in relation to Mediversal Generali Studium**	
What is the purpose of data processing?	Online healthcare appointment requests at the Controller for foreign students enrolled in Mediversal Generali Studium	
Who are the data subjects?	International students of the University of Szeged, who can be identified or have been identified on the basis of their data recorded on the website (https://mediversal.hu/generali-studium/)	
Who/what are the data sources?	The data subjects.	
What are the categories and scope of the data processed?	**What is the purpose of the various data categories?**	**What is the legal basis for processing?**
personal identification data (name, date of birth)	identification	prior and explicit consent (Article 6(1)(a) GDPR)
Generali Studium Card number	checks on free care	
contact details (phone number, e-mail address)	contact	
referral number (if applicable)	checks on free care	
uploaded data of the referring party		
comment	access to care	
indication of understanding and acknowledgement of the data protection policy	subsequent proof	legitimate interest of the Controller (Article 6(1)(f) GDPR)
date of submission		
What is the term of data processing?	The time and place provided by the Controller to the data subject (as a purpose) or, if the data subject has requested the erasure of his or her data, until erasure	
How is data processed?	The data subject enters his/her data on the above website, uploads his/her referral and, after having read the privacy policy, sends his/her data via a secure channel to the	

	Controller, who processes it and informs the data subject of the time and place.
Is data disclosed to third parties (by access, transfer, or forwarding)?	No.
Is a processor involved?	No.
Is there automated decision-making or profiling?	No.
Who are authorised to know the data?	The Controller's employees entrusted with the task.
Other information:	-

How does the Controller guarantee data security?

The Controller provides for data security. In the interest of the above, it takes those technical and organisational measures, and develops those procedural rules, that are necessary for ensuring compliance with the requirements or relevant legislation and data and confidentiality protection rules.

The Controller uses suitable measures to protect the data, thus from unauthorised access, alteration, forwarding, disclosure, deletion, destruction, unintentional destruction, damages, and inaccessibility due to changes to applied technologies.

The Controller also provides for the enforcement of the rules of data security by way of its internal regulations, instructions, and procedural orders.

When determining and applying the measures aimed at data security, it takes into account the state of the art of and, where alternate data processing solutions are available, the one selected shall ensure the highest level of protection of personal data, except if this would entail unreasonable hardship.

As regards its tasks involving IT security, the Controller shall especially ensure:

- the refusal of access to the tools used for data processing (hereinafter: data processing system) by unauthorised persons,
- the prevention of the unauthorised reading, copying, alteration, and removal of data media,
- the prevention of the unauthorised entry of personal data in the data processing system and the prevention of unauthorised access to and alteration and erasure of the personal data stored in the data processing system,
- the prevention of the use of the data processing systems by unauthorised persons using data transfer devices,
- that the persons authorised to use the data processing system can access only the personal data specified in their respective access permissions,
- that it is possible to verify and establish to which recipients personal data have been or may be transmitted or made available using data transfer devices,
- that it is possible to verify and establish subsequently which personal data have been entered into the data processing system and when and by whom,
- the prevention of the unauthorised access, copying, alteration, and erasure of the personal data in the course of their transfer or the transfer of any data media,
- that the data processing system can be restored following any faults,

- that the data processing system is operable, that reports are drawn up of any faults incurred in the course of operations, and that personal data cannot be altered even by way of the system's faulty operation.

What rights do data subjects have and how can they exercise those?

The following table shows the relationship between the data subject's rights and the respective legal basis, so that it is clear to the data subject what rights he or she can exercise under the applied legal basis.

	Right to prior information	Right of access	Right to rectification	Right to erasure	Restriction	Data portability	Right to object	Withdrawal of consent
Consent	✓	✓	✓	✓	✓	✓	✕	✓
Agreement	✓	✓	✓	✓	✓	✓	✕	✕
Legal obligation	✓	✓	✓	✕	✓	✕	✕	✕
Vital interest	✓	✓	✓	✓	✓	✕	✕	✕
Public task, public powers	✓	✓	✓	✕	✓	✕	✓	✕
Legitimate interest	✓	✓	✓	✓	✓	✕	✓	✕

Right of access (Article 15 GDPR)

The data subject shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information pertaining to the circumstances of data processing. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer. The Controller shall provide a copy of the personal data undergoing processing, if requested by the data subject.

Right to withdraw consent (Article 7 GDPR)

The data subject has the right to withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Right of rectification (Article 16 GDPR)

The data subject shall have the right to obtain, upon his or her request and without undue delay, the rectification by the Data Controller of inaccurate personal data relating to him or her.

Right to object (Article 21 GDPR)

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) GDPR.
The Controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

Right to restriction of processing (Article 18 GDPR)

The data subject shall have the right to obtain from the Controller restriction of processing where one of the following applies, in which case the Controller shall not perform any other action with the data besides storage.

The data subject has objected to processing pending the verification whether the legitimate grounds of the Controller override those of the data subject.

Right to erasure (right to be forgotten) (Article 17 GDPR)

The data subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay if the data processing has no purpose, the data subject has withdrawn consent and no other legal basis applies, in case of an objection, there is no overriding legitimate grounds for processing, if the data were originally processed unlawfully, or if the data must be erased to comply with a legal obligation. Where the Controller has made the personal data public and is obliged to erase the personal data, the Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Right to data portability (Article 20 GDPR)

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided, where the requirements specified by law (automated processing and consent or agreement legal basis) are met.

Where and how can the data subject request additional information on data processing and data transfer, and where and how can the data subject exercise its rights?

The Controller calls the attention of data subjects to the fact that data subjects may exercise their right to request information, right to access, and other rights by way of statements sent to the Controller's or the Data Protection Officer's mailing or email addresses. The Controller shall examine the statement and provide a reply within the shortest possible time following its receipt, and shall take the actions necessary based on the statement, the Internal Privacy Policy, and relevant legislation.

Contacting the authorities in case of a complaint (Article 77 GDPR):

Nemzeti Adatvédelmi és Információszabadság Hatóság [Hungarian National Authority for Data Protection and Freedom of Information]
Address: 1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1363 Budapest, Pf. 9.
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
www: http://www.naih.hu
email: ugyfelszolgalat@naih.hu

For additional information regarding your rights and the complaint to be submitted to the Authority, please visit the following website: http://naih.hu/panaszuegyintezes-rendje.html.

Data subjects whose rights have been violated may turn to a court of law with jurisdiction at their home address and may, among others, claim restitution.

You can find the court with jurisdiction at your home address here: https://birosag.hu/birosag-kereso

Mediversal Egészségügyi Szolgáltató Kft.
registered office: 6725 Szeged, Semmelweis u. 8.
company registration number: 06-09-011070
tax number: 13882495-2-06

The Controller reserves the right to amend this information.

Closed: 11 March 2023

Viktor Vaszari
Managing Director
Mediversal Kft.