PRIVACY POLICY

About the EKapu Application
(hereinafter referred to as the **"Policy"**)

Swiss Medical Services Kft. as data controller (hereinafter referred to as the ***"Controller"***) makes the in-house developed EKapu Application (hereinafter referred to as the ***"Application"***) available to Employers who have a contractual relationship with the Contoller, for the duration of the occupational health service contract, in order to improve the quality of its occupational health service. The Application is used to track the validity period of fitness-for-duty examinations, to notify the Employer, to summarise the examinations carried out and their results, to generate referrals, and to book examinations for their Employees by the Employer and for the Employees themselves. When using the Application, the Controller processes personal data of natural person employees using its healthcare services (hereinafter referred to as ***"Data Subjects"***) but does not process any health data when using the Application.

The personal data processed by the Controller may be accessed by persons working for the Controller (employees, contractors, etc.) only for the performance of their tasks and only to the extent necessary for the provision of occupational health or related services to the Data Subject, subject to the obligation of confidentiality.

With this Policy, the Controller intends to inform the Data Subjects about the scope of the personal data processed, the legal basis and purpose of the processing, the means and methods of processing and the measures taken to protect the data.

1. Definition of the Controller, personal data

The Controller is the legal person that determines, alone or jointly with others, the purposes and means of the processing of personal data. For the purposes of this Policy, personal data is any information relating to an identified or identifiable natural person, the Data Subject.

2. Subject of the Policy, legal basis for data processing

The subject of this Policy is the organisation of examinations of persons using the occupational health services of the Controller using the Application, the sending of the results of occupational health examinations and the recording of the results of occupational health examinations, in accordance with the applicable legislation.

Main legislation applicable to the processing of data under this Policy:

a) Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as *"GDPR"*)

b) the Act No. CXII of 2011 on Informational Self-Determination and Freedom of Information of Hungary

c) the Act No. XLVIII of 1997 on Processing for Personal Data Concerning Health of Hungary

d) the Ministerial Decree No. 62/1997 (XII. 21.) on certain aspects of the processing of health and related personal data

e) the Act No. XCIII of 2012 on Occupational Health and Safety

f) the Government Decree No. 89 of 1995 on Occupational Health Service (hereinafter referred as "Gov. Decree")

g) the Ministerial Decree No. 33 of 1998 on Assessment of Working Capacity, Employment Skills, and Suitability (hereinafter referred as "Min. Decree")

In preparing this Policy, we have taken into account the recommendation of the National Authority for Data Protection and Freedom of Information on the data protection requirements for prior information.

3. The legal basis of Data Controlling

According to the Article 6 (1) of GDPR processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

In view of the above, the primary legal basis for the Controller's processing is Article 6(1)(a), (b), (c) and (f) of the GDPR.

4. Data processing related to the use of the Application

Purpose of data processing	Organising the provision of health care services, fulfilling obligations under the occupational health contract, enforcing rights and maintaining contacts.
Legal basis of data processing	Performance of a health care contract, Article 6(1)(b) GDPR) Performance of a legal obligation, Article 6(1)(c) GDPR)
Scope of personal data concerned	Personal identification data (e.g. name, date of birth, mother's name) and contact details (address, telephone number, e-mail address), social security number (social security number), job title, if relevant for the provision of health services. Suitability opinion (which only states that the Data Subject as employee is suitable – not suitable – temporarily not suitable for employment). In using the Application, the Controller does not process any health data that is sensitive data.
Duration of processing; erasure	The duration of data processing corresponds to the general statute of limitations (limitation period – 5 years from the termination of the employment of the Data Subject or the termination of the legal relationship of the Controller with the employer), after which the data will be deleted or destroyed.
Recipient categories, data transfer	The Controller may transmit the personal data provided for the use of the Application to the authorities and courts specified by law, at their official request, on the basis of law.
Consequences of not providing data	The provision of data is necessary for the provision of the occupational health service, for the performance of the contract, and therefore, in case of failure to provide data, the service cannot be provided or cannot be provided properly.

5. Data security

The Controller is obliged to inform the Data Subjects about the processing of their personal data and to ensure the security of the personal data processed by the Controller. The Controller may disclose facts, data and opinions concerning the Data Subject to third parties only in cases specified by law or with the consent of the Data Subject.

The Controller shall, taking into account the state of science and technology and the costs of implementation, the nature, scope, circumstances and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, take all technical and organisational measures and establish the procedural rules necessary to ensure that the data recorded, stored or processed are protected and to prevent their destruction, unauthorised use or unauthorised alteration.

The Controller also undertakes to require all third parties to whom it transfers or discloses the data on whatever legal basis to comply with the requirement of data security.

The Controller shall also ensure that the processed data cannot be accessed, disclosed, transmitted, modified or deleted by unauthorised persons. The processed data may only be accessed by the Controller, its authorised employees and any data processor(s), according to the level of authorisation, and the Controller shall not disclose the data to third parties who are not authorised to access the data.

In order to ensure the security of its IT systems, the Controller protects its IT systems with a firewall, uses antivirus software to prevent external and internal data loss, and ensures that incoming and outgoing communications in any form are properly monitored to prevent misuse.

The Controller classifies and manages personal data as confidential and, in order to protect the data files managed electronically in different registers, ensures that the data stored in the registers cannot be directly linked and attributed to the Data Subject, subject to the exceptions provided for by law.

The Controller shall ensure a level of data security appropriate to the level of risk, including, where applicable: the pseudonymisation and encryption of personal data, the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data (operational and development security, intrusion protection and detection, prevention of unauthorised access), the ability to restore access to and availability of personal data in the event of a physical or technical incident in a timely manner (prevention of data leakage; vulnerability and incident management) and a procedure to regularly test, assess and evaluate the effectiveness of technical and organisational measures taken to ensure the security of data processing (business continuity, protection against malicious code, secure storage, transmission, processing of data, security training for its employees).

In determining the appropriate level of security, explicit account should be taken of the risks arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

6. Data processor(s)

Data Processor is a natural or legal person who processes personal data on behalf of the Controller. The Controller shall only use Data Processors who can provide adequate guarantees to ensure the obligations set out in this Policy. Data Processors are entitled to process personal data for the duration of their contract with the Controller or for the periods specified in the contract.

The Controller informs the Data Subjects that ACE Telecom Kft. (registered office: 1037 Budapest, Zay utca 3.; company registration number: 01-09-569352; tax number: 12255726-2-41; customer service telephone number: 1248; website: www.acetelecom.hu) acts as Data Processor in connection with the hosting of the Application.

7. Rights in relation to data processing and possibilities for enforcement and redress in relation to data processing

7.1. Rights in relation to data processing

The Data Subject may from the Controller

a) request information about the processing of his/her personal data (before the processing starts or during the processing);
b) request access to his or her personal data (the provision of his or her personal data by the controller);
c) request the rectification of his/her personal data;
d) request the erasure or restriction (blocking) of his or her personal data, except for mandatory processing;
e) exercise his or her right to data portability;
f) object to the processing of his/her personal data.

7.1.1. Right to information (Articles 13-14 GDPR)

The Data Subject may request information in writing from the Controller about the personal data processed, on what legal basis, for what purpose, from what source, for how long, whether a data processor is used, and if so, the name and address of the data processor and the data processing activities, to whom, when, under what law, to which personal data, to which personal data the Controller has granted access or to whom the Controller has transferred the personal data, the circumstances of any personal data breach, its effects and the measures taken to remedy it. The Controller shall respond to the Data Subject's request in writing to the contact details provided by the Data Subject within a maximum of one month.

7.1.2. Right to access (Article 15 GDPR)

The Data Subject has the right to receive feedback from the Controller as to whether or not his or her personal data are being processed and, if such processing is ongoing, the right to access the personal data processed. The Controller shall provide the Data Subject with a copy of the personal data which are the subject of the processing, unless there are other legal obstacles.

7.1.3. Right to rectification, completion (Article 16 GDPR)

The Data Subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. The Controller shall comply with the Data Subject's request within a maximum of one month and shall inform the Data Subject in writing at the contact details provided by the Data Subject.

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

The Data Subject may request in writing the erasure of his or her personal data by the Controller if the processing is based on the Data Subject's consent. If the processing of the Data Subject's personal data is already based on a legal ground, the Controller is entitled to refuse the erasure request and to process the data for the mandatory retention period. In the absence of mandatory retention, the Controller shall comply with the Data Subject's request within a maximum of one month and shall inform the Data Subject in writing at the contact details provided by the Data Subject.

7.1.5. Right to blocking (restriction of processing) (Article 18 GDPR)

The Data Subject may request in writing that his or her personal data be blocked by the Controller (by clearly indicating the limited nature of the processing and ensuring that it is kept separate from

other data). The blocking will last as long as the reason indicated by the Data Subject makes it necessary to store the data. For example, the Data Subject may request the blocking of data if he or she believes that the data have been unlawfully processed by the Controller, but the Controller is required not to delete the data in order to comply with the administrative or judicial procedure initiated by the Data Subject.

7.1.6. Right to data portability (Article 20 GDPR)

The Data Subject may request in writing that personal data relating to him or her which he or she has provided to the Controller be provided in a structured, commonly used, computer-readable format, and may also request the transfer of such data to another controller, provided that:

a) the processing is based on consent within the meaning of Article 6(1)(a) or Article 9(2)(a) GDPR;
b) based on a contract within the meaning of Article 6(1)(b) GDPR; and
c) the processing is carried out by automated means.

7.1.7. Right to object (Article 21 GDPR)

The Data Subject may object in writing to the processing of his or her personal data pursuant to Article 6(1)(f) of the GDPR, including profiling based on those provisions, necessary for the purposes of the legitimate interests pursued by the Controller or a third party. In such a case, the Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

7.2. Enforcement and remedies in relation to data management

7.2.1. Contacting the Controller

The Data Subject may contact the Controller's central contact details, the Controller's HR staff and the Data Protection Officer of the Controller if he or she has any questions or requests clarification regarding the data processed by the Controller. The Data Protection Officer of the Controller is Dr. Krisztina Vauver (postal address: 1062 Budapest, Andrássy út 113; telephone number: +36 1 451 1060; e-mail address: adatvedelem@swissclinic.hu)

The Controller shall, without undue delay, investigate the matter, take action on the request and provide information to the Data Subject in the event of the assertion of a right of the Data Subject in relation to data processing, a request for information in relation to data processing or a protest or complaint in relation to data processing, within the time prescribed by the applicable legislation. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended as provided for by law.

If the Data Subject has submitted the request by electronic means, the information shall be sent to him or her electronically, where possible, unless the Data Subject requests otherwise. If the Controller does not act on the Data Subject's request without delay, but at the latest within the time limit laid down by law, it shall inform the Data Subject of the reasons for the failure to act or the refusal to act and of the possibility for the Data Subject to take legal or administrative action in accordance with the following.

7.2.2. Initiation of legal proceedings

The Data Subject may take legal action against the Controller or its processor if he or she considers that the Controller or a processor acting on his or her behalf or under his or her instructions is processing his or her personal data in breach of the provisions on the processing of personal data laid down by law or by a legally binding act of the European Union. A court of law shall have jurisdiction and may, at the Data Subject's option, be seized before the competent court in the place where the Data Subject resides or is domiciled.

The Controller shall compensate the damage caused by the unlawful processing of the Data Subject's data or by the breach of data security requirements but shall be exempt from liability if the damage was caused by an unavoidable cause outside the scope of the processing or if it resulted from the intentional or grossly negligent conduct of the Data Subject.

7.2.3. Initiation of an administrative procedure

The Data Subject may lodge a complaint with the National Authority for Data Protection and Freedom of Information (registered office: 1055 Budapest, Falk Miksa utca 9-11.; website: http://naih.hu; postal address: 1363 Budapest, Pf. ; telephone number: +36 1 391 1400; e mail: ugyfelszolgalat@naih.hu) may initiate an investigation or an official procedure to enforce his or her rights on the grounds that his or her personal data are being processed in a way that adversely affects or threatens to adversely affect his or her rights, in particular if he or she considers that the Controller is restricting the exercise of his or her rights or is refusing his or her request to exercise those rights (initiation of an investigation), and if he or she considers that the processing of his or her personal data by the Controller or by a processor appointed or instructed by the Controller or by a processor acting on his or her behalf infringes the provisions on the processing of personal data laid down by law or by a legally binding act of the European Union (request for a public authority procedure).

8. Miscellaneous

No automated decision-making, profiling or transfer of personal data to a third country or international organisation will take place in the processing of personal data detailed in this Policy.

The Controller reserves the right to unilaterally amend this Policy in the future. The Data Subjects will be informed of such changes via the Controller's website.