PRIVACY POLICY

Regarding Medical and Occupational Health Services
(hereinafter: **Privacy Policy**)

The companies belonging to the Swiss Clinic group, as listed in Annex 1 and acting as Data Controllers (hereinafter: Data Controller or Data Controllers), process the personal data of natural persons (hereinafter: Data Subjects) who use their healthcare and occupational health services during the provision of such services. **Below, they provide information on the management of these personal data** for other Data Subjects.

Introduction

When a private individual wishes to use the services of any of the Data Controllers, or when their employer or prospective employer orders an occupational health examination from any of the Data Controllers to assess work suitability, or if the employer orders any health service from the Data Controllers for the Data Subject, certain personal data of the Data Subjects are provided either by the Data Subject or their employer. With this Privacy Policy, we aim to inform Data Subjects about the categories of personal data processed, the legal basis and purpose of the data processing, the tools and methods used, the circumstances, and the measures we have taken to protect the data.

The concept of personal data processing includes any operation or set of operations performed on personal data, such as recording, storing, accessing, using, disclosing, transferring, deleting, or destroying. In processing personal data, the Data Controllers take all necessary and appropriate measures to prevent unauthorized access to and unauthorized use of personal data. As part of this, they ensure the physical security of their facilities (such as operating entry and camera systems) and protect their systems against unauthorized access (e.g., by using firewalls, two-factor authentication, and NIS2 accreditation).

Persons working for the Data Controllers (employees, contributors, etc.) may have access to the personal data managed by the Data Controllers solely for the performance of their tasks and only to the extent necessary to provide healthcare or related services to the Data Subject and are bound by a duty of confidentiality.

It may occur that the Data Controllers transfer the data they process to third parties (e.g., to authorities or to fulfill legal obligations, such as uploading to the general data base on health-related data i.e. EESZT). Data may also be transferred for the purpose of providing services to the Data Subject, or if the Data Controllers use third-party data processors for certain processing operations (e.g., data storage, organization), in which case the Data Controllers require appropriate guarantees from these third parties to ensure the protection set out in this Privacy Policy.

1. Definition of Data Controllers and Personal Data

The Data Controller is the legal entity that **individually or jointly with others determines the purposes and means of processing personal data**. For the purposes of this Privacy Policy, the data controller(s) is the legal entity listed in Annex 1 that provides the respective occupational health or other healthcare service. Regarding the data processing covered by this Privacy Policy, the Data Controllers **are not considered joint controllers** under Article 26 of the GDPR; the Data Controllers are independent data controllers who determine the purposes and means of their own data processing independently.

For the purposes of this Privacy Policy, personal data means any information relating to an identified or identifiable natural person, the Data Subject. An identifiable natural person is one who can be identified,

directly or indirectly, in particular by reference to an identifier (such as name, number, identification, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person).

2. Subject of the Privacy Policy, Legal Basis for Data Processing

This Privacy Policy applies to the provision of healthcare services by the Data Controller to individuals, and includes registration on websites, appointment scheduling, the processing of the Data Subject's personal and health data, the organization of occupational health examinations, the organization of specialist medical examinations, the sending and recording of examination results, all in accordance with the relevant legal regulations.

The main laws governing the data processing covered by this Privacy Policy and their abbreviations as used in this Privacy Policy are as follows:

a) Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 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 (GDPR)

b) Act CXII of 2011 on the right of informational self-determination and freedom of information (Infotv.)

c) Act XLVII of 1997 on the management and protection of health and related personal data;

d) Decree 62/1997 (XII. 21.) NM on certain issues of the management of health and related personal data;

e) Act CLIV of 1997 on healthcare (hereinafter: Eütv.);

f) Act XCIII of 1993 on occupational safety and health;

g) Government Decree 89/1995 (VII. 14) on the organization and operation of occupational health services and the classification of employees by category;

h) Decree 33/1998 NM on the medical examination and assessment of job, professional, and personal hygiene suitability;

i) Provisions set out in Article VI, points 3-4 of the Fundamental Law of Hungary;

j) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (AI Act)

In preparing this Privacy Policy, we took into account the recommendations of the National Authority for Data Protection and Freedom of Information (NAIH) on the requirements of prior information in data protection, and this Privacy Policy also serves the obligation of written information to the Data Subject as required by Section 10 (5) of the Labor Code (Mt.).

3. Legal Bases for the Data Controller's Data Processing

Article 6(1) of the GDPR, which states that the processing of personal data is 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 their personal data for one or more specific purposes;

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

The Data Controller may require the Data Subject to make only such statements or disclose only such personal data as are essential for the establishment, performance, termination (cessation) of an employment or other legal relationship, or for enforcing employment-related claims. The Data Controller may require presentation of documents to verify the personal data provided.

The Data Subject may be subject to such aptitude tests as are prescribed by regulations relating to employment, or as are necessary for the exercise of rights or fulfilment of obligations defined in employment-related regulations.

4. Types of Data Processing

For the purposes of this Privacy Policy, medical treatment is defined as any activity aimed at preserving health, as well as preventing, detecting early, diagnosing, or healing diseases, maintaining or improving a condition that has deteriorated due to illness, through direct examination, treatment, nursing, or medical rehabilitation of the Data Subject, and, for these purposes, the processing of the Data Subject's test samples, including the supply of medicines, medical aids, and medical care.

A health data is any personal data concerning the Data Subject's physical or mental health, including any data relating to health services provided to the Data Subject that contains information about the Data Subject's condition.

This includes any personal data relating to the Data Subject's past, present, or future physical or mental health, which have been collected for the purpose of registering for or providing health services; any number, symbol, or data assigned to the Data Subject for identification for health purposes; information derived from the testing or examination of any bodily part or material constituting the body—including genetic data and biological samples; and any information, for example, related to the Data Subject's illness, disability, risk of disease, medical history, clinical treatment, or physiological or medical condition, regardless of its source, which may be, for example, a physician or other healthcare worker, hospital, medical device, or in vitro diagnostic test.

Health-related personal data include data on health status (laboratory diagnostic results, diagnoses of certain diseases, genetic data, etc.), as well as data that refer to the health service used and from which information about the health status can also be inferred (for example, data on whether the person attended a particular treatment or provider).

Health data are considered special categories of data.

Health and personal identification data are provided by the Data Subject voluntarily—except for identification data that are mandatory for accessing healthcare services and in cases defined by law, such as epidemiological matters, poisoning, certain occupational diseases, the treatment, preservation, or protection of the health of a fetus or minor child, or data transfers required for law enforcement or national security purposes.

Subject to the Data Subject's prior consent, the purpose of the data processing is to enable the Data Controller to use artificial intelligence (hereinafter: AI) to optimize the level of patient safety, as well as the duration of the doctor-patient relationship (by reducing the time spent on administrative tasks while increasing the time spent on the Data Subject's care), and educational purposes are also associated with the data processing. AI does not make or suggest any decisions on behalf of the attending physician. AI may be used in the following cases:

Use Case	Essence of the use
Speech Recognition Application Assisting the Writing of Medical Documentation	The application allows the physician to dictate medical documentation, which is converted into text by the AI through multiple verification steps. The physician is required to review the finalized text. **The application does not involve the processing of personal data**; the physician only dictates the circumstances and characteristics of the case.
Medical Report Summary Application	It is designed to process findings and laboratory results, as well as to produce a medically relevant summary of them. It is particularly helpful for the physician when handling a large volume of documentation. The physician is required to review the summary.
Drug Interactions and Interaction Analysis	The AI, **without processing personal data**, compares the Data Subject's current medication and test results in real time with medical protocols. The system's task is to identify and indicate potential drug interactions, contraindications, and lifestyle risks (such as specific dietary effects). The physician is required to review the outcome.

The application of the above functions (uses) is subject to the condition that the attending physician must inform the Data Subject in advance and request their consent. Refusing consent in no way affects the provision of care.

4.1. Data Processing Related to the Provision of Health and Occupational Health Services, and the Fulfillment of Contracts for Health Care Services

Purpose of Data Processing	Provision of healthcare services, conclusion, modification and termination of a contract for such services, fulfillment of contractual obligations, enforcement of rights and any claims, defense against claims, fulfillment of legal obligations, and maintaining contact.
Legal Basis of Data Processing	Performance of a contract for healthcare services, GDPR Article 6(1)(b) Fulfillment of legal obligations, GDPR Article 6(1)(c) Legitimate interest in enforcing claims, GDPR Article 6(1)(f) Consent under GDPR Article 6(1)(a) regarding the use of AI.

	The processing of special categories of data is possible under GDPR Article 9(2)(h), and in certain cases, under Article 9(2)(a) (healthcare exception, or the data subject's consent).
Scope of Personal Data Concerned	Personal identification data (e.g.: name, date of birth, mother's name), contact details (address, mailing address, phone number, email address), health data generated in connection with the provision of healthcare, as well as social security number (TAJ number), and for persons insured under a group health insurance policy provided by a health insurance provider, workplace, insurance package. Occupation, religious belief, and racial origin, if relevant to the provision of healthcare services.
Source of Data	The above personal data are partly provided by the Data Subject, partly obtained by the Data Controller from other healthcare providers with the Data Subject's consent, and in the case of occupational health services, the employer, as the Data Controller's client, forwards the necessary personal identification and contact details for occupational health examination.
Duration of Data Processing; Deletion	Based on Act XLVII of 1997 on the processing and protection of health and related personal data, the Data Controller retains all healthcare and personal identification data forming part of the healthcare documentation for 30 years from the date of data collection, discharge summaries for 50 years, and diagnostic imaging records for 10 years from their creation. After these deadlines, healthcare documentation containing personal data will be deleted or destroyed.
Categories of Recipients, Data Transmission	The Data Controller transmits personal data to the following recipients: (i) To healthcare service provider partners for the provision of healthcare services, fulfillment of contract, and for necessary activities (e.g.: laboratory tests, emergency care, certain specialized services); (ii) To authorities defined by law, for the fulfillment of reporting obligations (e.g. epidemiological reporting in case of infectious disease); (iii) To authorities and courts defined by law, upon their official request or summons, as provided for by law; (iv) To its data processor providing document archiving and record storage services, based on a data processing agreement; (v) To its data processor providing server services, based on a data processing agreement; (vi) To delivery companies acting as data processors, the data necessary for delivery (name and address), based on a data processing agreement.
Consequence of Failure to Provide Data	Providing data is necessary for the provision of healthcare services and fulfillment of the contract, so if data is not provided, the service cannot be provided or can only be provided inadequately.

4.2. Recording of Telephone Conversations (Call Centre)

Purpose of Data Processing	The general purpose of recording telephone conversations is to provide evidence of what was said during the call. In the case of complaints made by phone, the aim is to accurately record and document the complaint. An

	additional purpose is the continuous improvement of the Data Controller's services.
Legal Basis for Data Processing	The legal basis for data processing is the Data Subject's consent, which is given by continuing the call after being informed of the recording (GDPR Article 6(1)(a)). Additionally, the Data Controller's legitimate interest in quality assurance and enforcing claims (GDPR Article 6(1)(f)).
Scope of Personal Data Concerned	The Data Subject's voice, any personal data disclosed during the initiated and ongoing telephone conversation, the date and time of the call, its duration, and the caller's number.
Duration of Data Processing; Deletion	The duration of data processing corresponds to the statute of limitations (claim enforcement period—5 years from the end of the call, or in the case of complaints, from the closure of the complaint case), after which the data is deleted or destroyed.
Categories of Recipients, Data Transmission	The Data Controller may transmit the personal data provided during the telephone conversation to authorities or courts defined by law, upon their official request or summons, or as required by legislation.
Consequence of Failure to Provide Data	Without the necessary data, complaints submitted by telephone cannot be handled or can only be handled inadequately. In other cases, if personal data is not provided, the Data Subject's request cannot be fulfilled and their queries cannot be answered.

4.3. Data Processing Related to Complaint Handling

Purpose of Data Processing	The purpose of data processing related to complaint handling is to investigate the complaint, clarify its circumstances, and ensure the continuous improvement of the quality of the Data Controllers' services.
Legal Basis for Data Processing	Performance of the occupational health contract or other contract, GDPR Article 6(1)(b) Fulfilling the legal obligation related to complaint handling as stipulated by Act CLIV of 1997 on Healthcare, GDPR Article 6(1)(c) The Data Subject's consent, given by submitting the complaint to the Data Controller, GDPR Article 6(1)(a)
Scope of Personal Data Processed	Personal identification data provided in the complaint by the complainant (typically: name, e-mail address, home address), as well as any personal, potentially health-related data included in the complaint.
Duration of Data Processing; Deletion	According to Act CLIV of 1997 on Healthcare, the duration of data processing is five years from the closure of the complaint case, after which the data will be deleted or destroyed.
Categories of Recipients, Data Transfers	The Data Controller forwards the personal, and if applicable, health-related data relating to complaints to the following recipients: (i) to partner healthcare service providers, for the purpose of investigating the circumstances of the healthcare service affected by the complaint; (ii) to authorities and courts specified by law, upon their official request or summons, based on statutory provisions;

	(iii) to its data processor providing document archiving and record storage services, based on a data processing agreement; (iv) to companies delivering consignments, as data processors, only the data necessary for delivery (name and address), based on a data processing agreement. (v) in the case of a person insured by a health insurance provider, to the insurer or employer, if the complaint was submitted through either of them and the Data Subject has consented to the forwarding of their personal data to the insurer or employer in relation to complaint handling.
Consequence of Failure to Provide Data	All essential data related to the complaint are necessary for the handling of the complaint and investigation of circumstances. Failure to provide data, or incomplete data provision, may result in the complaint not being handled or not being handled appropriately.

4.4. Data Processing in Connection with Communication and Other Inquiries

Purpose of Data Processing	The purpose of data processing is communication, fulfillment of contracts, provision of services, collection and evaluation of feedback related to the quality of services, and responding to questions raised by the Data Subjects. Another purpose is the continuous improvement of the quality of the Data Controllers' services.
Legal Basis for Data Processing	In the case of occupational health service contracts and other contracts, the legal basis for processing the personal data of the contacts specified in the contract is the legitimate interest of fulfilling the contract, Article 6 (1) (f) of the GDPR. For other notifications, inquiries, questions, or participation in customer satisfaction surveys, the legal basis is the Data Subject's consent, provided by submitting the given notification, inquiry, or question, or by completing the questionnaire, Article 6 (1) (a) of the GDPR.
Categories of Personal Data Concerned	Personal identification data provided for contact purposes (typically: name, email address, home address), as well as personal data, and where applicable, health data included in the customer satisfaction survey.
Duration of Data Processing; Deletion	For contractual contacts, the duration of data processing is from the termination of the contract; in other cases, the duration is 5 years from the receipt of the inquiry, after which the data will be deleted or destroyed.
Categories of Recipients, Data Transfers	The Data Controller forwards the personal data related to communication to the following recipients: (i) to authorities and courts specified by law, upon their official request or summons, based on statutory provisions; (ii) to its data processor providing document archiving and record storage services, based on a data processing agreement.
Consequence of Failure to Provide Data	If the provision of data is omitted or incomplete, communication is not possible.

4.5. Data Processing Related to Newsletter Services

Purpose of Data Processing	The purpose of data processing is to promote the Data Controllers' services, facilitate their use, and acquire new business.
Legal Basis for Data Processing	The Data Subject's consent, Article 6 (1) (a) of the GDPR The legitimate interest of the Data Controllers in promoting their services, Article 6 (1) (f) of the GDPR
Categories of Personal Data Concerned	Personal identification data provided for contact purposes (name, email address).
Duration of Data Processing; Deletion	The duration of data processing is aligned with consent; after withdrawal of consent or objection to data processing, the data will be deleted immediately, but no later than within 30 days.
Categories of Recipients, Data Transfers	The Data Controller forwards personal data related to communication to the following recipients: to authorities and courts specified by law, upon their official request or summons, based on statutory provisions.
Consequence of Failure to Provide Data	If the provision of data is omitted or incomplete, the newsletter service cannot be provided.

4.6. Data Processing Related to Social Media Accounts

Purpose of Data Processing	The purpose of data processing is to operate the Data Controllers' social media profiles, promote their services, facilitate their use and business acquisition, as well as to improve their quality.
Legal Basis for Data Processing	The Data Subject’s consent by creating the given social media account and by visiting the Data Controllers’ social media profiles, Article 6 (1) (a) of the GDPR The legitimate interest of the Data Controllers in operating their social media profiles, Article 6 (1) (f) of the GDPR
Categories of Personal Data Concerned	Personal identification data provided by the Data Subject as a user when creating the social media account and later, as well as other information published by them.
Duration of Data Processing; Deletion	The duration of data processing is the general limitation period, 5 years.
Categories of Recipients, Data Transfers	The Data Controller will only transfer personal data obtained in connection with social media accounts to authorities in the case of suspected criminal offenses linked to the specific social media account.
Consequence of Failure to Provide Data	There are no consequences for failure to provide data.

5. Data Security

The Data Controller is obligated to inform Data Subjects about the processing of their personal data and to ensure the security of the personal data it processes. The Data Controller may only disclose facts,

data, or opinions concerning the Data Subject to third parties in cases defined by law or with the Data Subject's consent.

Taking into account the state of science and technology, the costs of implementation, the nature, scope, circumstances, and purposes of data processing, as well as the varying probability and severity of risks to the rights and freedoms of natural persons, the Data Controller shall take all technical and organizational measures and establish those procedural rules that ensure that the data collected, stored, or otherwise processed are protected and that their destruction, unauthorized use, and unauthorized modification are prevented.

The Data Controller also undertakes to call upon all third parties to whom it transmits or transfers data on any legal basis to comply with the requirements of data security.

The Data Controller shall also ensure that unauthorized persons cannot access, disclose, transfer, modify, or delete the processed data. The processed data may only be known to the Data Controller, its authorized employees, and any data processors engaged, according to their levels of authorization; the Data Controller does not transfer the data to any third party not authorized to access them.

To ensure the security of IT systems, the Data Controller protects IT systems with a firewall, uses antivirus and anti-malware software to prevent both external and internal data loss, and ensures that all incoming and outgoing communications are properly monitored to prevent abuse.

The Data Controller classifies and handles personal data as confidential and, in order to protect electronically managed data files in various registers, ensures that the data stored in these registers—except in cases defined by law—cannot be directly linked or assigned to the Data Subject.

The Data Controller guarantees a level of data security appropriate to the degree of risk, including but not limited to: pseudonymization and encryption of personal data, ensuring the ongoing confidentiality, integrity, availability, and resilience of systems and services used to process personal data (operational and development security, protection against and detection of intrusions, prevention of unauthorized access), the ability to restore access to personal data and their availability in a timely manner in the event of a physical or technical incident (prevention of data leakages; vulnerability and incident management), and procedures for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing (business continuity, protection against malicious code, secure storage, transmission and processing of data, and security training for our Data Subjects).

When determining the appropriate level of security, particular attention must be paid to the risks arising from data processing, especially those resulting from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

6. Recipients of Data Transfers

6.1. Independent Data Controllers

Members of the Swiss Clinic group process personal data as described in this Privacy Policy as independent Data Controllers, based on their legitimate interest. Group members are only entitled to transfer data as described in this Privacy Policy for the purpose of group-level HR activities.

6.2. Data Processors

A data processor is a natural or legal person who processes personal data on behalf of the Data Controller. The Data Controllers only use Data Processors who can provide adequate guarantees to ensure the obligations set out in this Privacy Policy are met. Data Processors are entitled to process

personal data during the term of their contract with the Data Controller, or for the periods specified in the contract.
The Data Controller informs Data Subjects that, as a Data Processor, in connection with

(i) imaging diagnostic examinations performed at Swiss Buda Premium Health Center (1123 Budapest, Nagyenyed utca 8.) **B Radiológiai Centrum Kft.** (registered office: 1123 Budapest, Nagyenyed utca 8.),

(ii) and for laboratory tests in all facilities, **SYNLAB Hungary Kft.** (registered office: 1211 Budapest, Weiss Manfréd út 5-7.),

(iii) for cytological and histological laboratory examinations, **MEDSERV Egészségügyi, Szolgáltató és Kereskedelmi Kft.** (registered office: 1047 Budapest, Fóti út 56. A building),

(iv) and for remote X-ray reporting, **ICONOMIX Kft.** (registered office: 7626 Pécs, Koller utca 9. B building, ground floor 5.) acts as Data Processor.

(v) For the use of AI, **Genova Labor Magyarország Kft.** (registered office: 1121 Budapest, Tállya utca 6. B building) is involved. No other data transfers take place.

7. Rights Related to Data Processing and Legal Remedies

7.1. Rights Related to Data Processing

The Data Subject may, from the Data Controller:

(vi) request information about the processing of their personal data (before and during data processing);

(vii) request access to their personal data (having their personal data made available by the Data Controller);

(viii) request the rectification or supplementation of their personal data;

(ix) request the erasure or restriction (blocking) of their personal data – except for mandatory data processing;

(x) exercise their right to data portability;

(xi) object to the processing of their personal data.

7.1.1. Right to Information (GDPR Articles 13–14)

The Data Subject may request in writing from the Data Controller information about what personal data is processed, on what legal basis, for what purpose, from what source, and for how long, whether a data processor is used, and if so, the name, address, and activities of the processor, to whom, when, and on what legal basis the Data Controller has provided access to or forwarded the personal data, and information about any data protection incidents, their effects, and measures taken to address them. The Data Controller will fulfill the Data Subject's request in writing within a maximum of one month, sent to the contact information provided by the Data Subject.

7.1.2. Right of Access (GDPR Article 15)

The Data Subject is entitled to receive feedback from the Data Controller as to whether their personal data is being processed, and if so, to access the personal data being processed. The Data Controller will provide a copy of the personal data undergoing processing to the Data Subject—provided this does not conflict with other legal prohibitions.

7.1.3. Right to Rectification and Completion (GDPR Article 16)

The Data Subject may request in writing to the Data Controller the modification of any of their personal data (e.g., they may change their contact details or request that any inaccurate personal

data managed by the Data Controller be corrected). Considering the purpose of data processing, the Data Subject is entitled to request the appropriate supplementation of any incomplete personal data managed by the Data Controller. The Data Controller will fulfill the Data Subject's request within a maximum of one month and will inform the Data Subject in writing at the contact details provided.

7.1.4. Right to Erasure ("Right to be Forgotten") (GDPR Article 17)

The Data Subject may request in writing that the Data Controller delete their personal data 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 Data Controller is entitled to refuse the erasure request and to continue processing the data for the mandatory retention period. If there is no mandatory retention, the Data Controller will fulfill the Data Subject's request within a maximum of one month and will inform the Data Subject in writing at the contact details provided.

7.1.5. Right to Restriction of Processing (GDPR Article 18)

The Data Subject may request in writing that the Data Controller restrict their personal data (by clearly indicating the restricted nature of processing and ensuring separation from other data). Restriction lasts as long as the reason identified by the Data Subject makes storage necessary. For example, the Data Subject may request restriction if they believe the Data Controller has processed the data unlawfully, but retaining the data is necessary for initiating official or judicial proceedings.

7.1.6. Right to Data Portability (GDPR Article 20)

The Data Subject may request in writing that personal data concerning them, which they have provided, be delivered by the Data Controller in a structured, commonly used, machine-readable format, and is also entitled to request that this data be transferred to another controller, provided that:

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

7.1.7. Right to Object (GDPR Article 21)

The Data Subject may object in writing to the processing of their personal data that is necessary for the legitimate interests of the Data Controller or a third party under Article 6(1)(f) of the GDPR, including profiling based on these provisions. In such cases, the Data Controller will not process the personal data further, unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the Data Subject, or are necessary for the establishment, exercise, or defense of legal claims.

7.2. Legal Remedies and Enforcement Options Related to Data Processing

7.2.1. Contacting the Data Controller

If the Data Subject has any questions concerning the data managed by the Data Controller, or seeks information regarding their data, they may do so by contacting the Data Controller's HR staff or the Data Protection Officer. The Data Protection Officer and their contact details are listed in Annex 1 of this Privacy Policy.

If the Data Subject exercises any right related to data processing, requests information, objects to processing, or submits a complaint, the Data Controller investigates the matter without undue delay and takes action within the timeframe prescribed by the applicable laws, and informs the Data

Subject of the outcome. If necessary, considering the complexity of the request and the number of requests, this deadline may be extended as provided by law.

If the Data Subject submitted their request electronically, the response should be provided electronically whenever possible, unless the Data Subject requests otherwise. If the Data Controller does not take action based on the Data Subject's request without delay, but at the latest within the period defined by law, the Data Subject will be informed of the reasons for the inaction or refusal and of the possibility to initiate judicial or administrative proceedings as described below.

7.2.2. Initiating Court Proceedings

The Data Subject may turn to a court against the Data Controller or its data processor if, in their opinion, the Data Controller or the data processor acting on behalf of or according to the instructions of the Data Controller processes their personal data in violation of the data protection regulations prescribed by law or mandatory legal acts of the European Union. The case falls within the jurisdiction of the regional court and may also be brought, at the Data Subject's choice, before the regional court competent for the Data Subject's place of residence or stay.

The Data Controller is required to compensate for any damage caused by the unlawful processing of the Data Subject's data or by violating data security requirements but is exempt from liability if the damage was caused by an unavoidable reason outside the scope of data processing or resulted from the Data Subject's intentional or grossly negligent conduct.

7.2.3. Initiating Administrative Proceedings

The Data Subject may request an investigation or administrative procedure from the National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa u. 9-11., website: http://naih.hu; mailing address: 1363 Budapest, Pf.: 9.; phone: +36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu) in order to enforce their rights, referring to a violation or imminent risk of violation related to the processing of their personal data, especially if they believe the Data Controller restricts the exercise of their rights or refuses their request for the exercise of such rights (initiation of an investigation), or if, in their opinion, the Data Controller or its data processor acting on its behalf or according to its instructions, violates the data protection regulations prescribed by law or mandatory legal acts of the European Union (request for initiation of administrative procedure).

8. Other Provisions

During the processing of personal data detailed in this Privacy Policy, no automated decision-making, profiling, nor transfer of personal data to third countries or international organizations takes place.

This Privacy Policy is available on the website of the Data Controller.

The Data Controller reserves the right to unilaterally amend this Privacy Policy with future effect. Data Subjects will be informed of any changes via the Data Controller's website. Unless otherwise specified, the amendments shall take effect immediately. Please check this Privacy Policy regularly to ensure that you are familiar with the current version.

Status: June 1, 2026

ANNEX 1

The Data Controllers and the Data Protection Officer

Members of the Swiss Clinic Group as Data Controllers / Controllers

SWISS MEDICAL SERVICES Korlátolt Felelősségű Társaság
Registered office: 1092 Budapest, Kinizsi utca 22. ground floor 4.
Company registration number: 01-09- 561648
Tax number: 12171864-2-43
Statistical code: 12171864-8622-113-01

SWISS MEDICAL HUNGARY Zártkörűen Működő Részvénytársaság
Registered office: 1125 Budapest, Táltos utca 15/B 2nd floor 1.
Company registration number: 01-10- 46809
Tax number: 22989143-2-43
Statistical code: 22989143-8622-114-01

SWISS EMERGENCY SERVICES Korlátolt Felelősségű Társaság
Registered office: 1113 Budapest, Ibrahim utca 26. 1st floor 103.
Company registration number: 01-09- 293357
Tax number: 25865370-1-43
Statistical code: 25865370-8621-113-01

The data protection officer for the above companies:

Dr. Krisztina Vauver
Mailing address: 1062 Budapest, Andrássy út 113.
Phone number: +36 1 451 1060
Email address: adatvedelem@swissclinic.hu