

Data Processing Agreement (DPA) including Standard Contractual Clauses (SCC)

(Articles 28 and 29 of the GDPR)

- Date: 15 August 2025 –

Preamble:

This Data Processing Agreement governs the rights and obligations of the parties in relation to the processing of personal data on behalf of the data controller in accordance with Article 28 of the GDPR. The content of this agreement is essentially based on the **Standard Contractual Clauses for the transfer of personal data to third countries in accordance with Implementing Decision (EU) 2021/914 of the European Commission of 4 June 2021**.

The Standard Contractual Clauses form the main body of this agreement and have been supplemented in accordance with the European Commission's guidelines by specific, contractually necessary additions – in particular by details regarding the technical and organisational measures, the nature of the data processed, the purposes of the processing, and the parties involved and sub-processors.

This agreement applies to all processing activities in connection with the service agreement concluded between the parties, in which employees of the Contractor or sub-processors commissioned by the Contractor process the Client's personal data ("Data") on the Client's behalf.

The terms used in this agreement are to be understood in accordance with the definitions set out in the EU General Data Protection Regulation ("GDPR").

1. Purpose and scope

- 1.1. These standard contractual clauses (hereinafter 'the clauses') are intended to ensure compliance with Article 28(3) and (4) of 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).
- 1.2. The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and Article 29(3) and (4) of Regulation (EU) 2018/1725.
- 1.3. These clauses apply to the processing of personal data as set out in Annex I.
- 1.4. Annexes I to IV form an integral part of these clauses.
- 1.5. These clauses apply without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679.

- 1.6. These clauses do not, in themselves, ensure that the obligations relating to international data transfers under Chapter V of Regulation (EU) 2016/679 are fulfilled.

2. Non-modification of the clauses

- 2.1. The parties undertake not to amend the clauses, except to supplement or update the information set out in the annexes.
- 2.2. This shall not prevent the parties from incorporating the standard contractual clauses set out in these clauses into a more comprehensive contract and from adding further clauses or additional guarantees, provided that these do not directly or indirectly conflict with the clauses or curtail the fundamental rights or freedoms of the data subjects.

3. Interpretation

- 3.1. Where terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 are used in these clauses, such terms shall have the same meaning as in the relevant Regulation.
- 3.2. These clauses shall be interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- 3.3. These clauses must not be interpreted in a manner that conflicts with the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, or that restricts the fundamental rights or freedoms of data subjects.

4. Precedence

- 4.1. In the event of any conflict between these clauses and the provisions of related agreements existing between the parties or entered into or concluded subsequently, these clauses shall prevail.

5. Accession clause

- 5.1. An organisation that is not a party to these clauses may, at any time, accede to these clauses as a controller or a processor, subject to the consent of all parties, by completing the annexes and signing Annex I.
- 5.2. Upon completion and signing of the annexes referred to in clause 5.1, the acceding entity shall be treated as a party to these clauses and shall have the rights and obligations of a controller or a processor in accordance with its designation in Appendix II.
- 5.3. No rights or obligations arising from these clauses shall apply to the acceding entity for the period prior to its accession as a party.

6. Subject matter and duration of the contract

- 6.1. The contract covers the following: processing of therapy data
- 6.2. The processor shall process personal data only for the specific purposes set out in Annex I, unless it receives further instructions from the controller.
- 6.3. In doing so, the contractor processes personal data on behalf of the client within the meaning of Article 4(2) and Article 28 of the GDPR.
- 6.4. The data shall be processed by the data processor only for the duration specified in Annex I.
- 6.5. Subject to the provisions of any existing main contract, any termination must be in writing.

7. Scope of processing / nature and purpose of processing

- 7.1. The Contractor processes personal data as follows and for the following purpose:
 - a) Storing and visualising device-specific and non-device-specific therapy data assigned to a user (patient)
- 7.2. Nature of the personal data and categories of data subjects
 - a) The nature of the data and the categories of data subjects covered by this agreement are defined in Annex I: Nature of the data and categories of data subjects.

8. Technical and organisational measures

- 8.1. The Contractor must document the implementation of the necessary technical and organisational measures set out prior to the award of the contract before processing begins, in particular with regard to the specific execution of the contract, and must submit the documentation to the Client for review. Upon acceptance by the Client, the documented measures shall form the basis of the contract. If the Client's review reveals a need for adjustments, these shall be implemented by mutual agreement.
- 8.2. The Contractor shall establish and ensure security in accordance with Article 28(3)(c) and Article 32 of the GDPR, in particular in conjunction with Article 5(1) and (2) of the GDPR. Overall, the technical and organisational measures to be taken in this context are data security measures designed to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In doing so, account must be taken of the state of the art, the costs of implementation and the nature, scope and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32(1) of the GDPR.
- 8.3. The details of the Contractor's technical and organisational measures (TOMs) are set out in Annex IV.

8.4. The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative, adequate measures. However, the level of security provided by the specified measures must not be compromised. Any significant changes must be documented.

9. Place of processing

9.1. The processing of data shall take place in a Member State of the European Union or in another State party to the Agreement on the European Economic Area.

9.2. Any transfer of data to another country (a so-called 'third country') requires the prior consent of the Client and may only take place if the specific requirements of Articles 44 et seq. of the GDPR are met.

10. Instructions and the authority to issue instructions to the processor

10.1. The processor shall process personal data only on documented instructions from the controller, unless it is required to do so by Union law or the law of a Member State to which it is subject. In such a case, the processor shall inform the controller of those legal requirements prior to processing, unless the law in question prohibits this on grounds of an important public interest. The controller may issue further instructions throughout the duration of the processing of personal data. These instructions shall always be documented.

10.2. The processor shall inform the controller without delay if it considers that instructions issued by the controller infringe Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or applicable data protection provisions of the Union or the Member States.

10.3. The processor shall not rectify, erase or restrict the processing of the data processed on behalf of the controller on its own initiative, but only within the framework of the agreements made or in accordance with documented instructions from the controller. Additions to the clauses are generally permissible, provided they clarify the content and do not weaken it, and must be recorded as an addendum or separate clause.

11. Security of processing

11.1. The processor shall implement at least the technical and organisational measures set out in Annex IV to ensure the security of the personal data. This includes protecting the data against a breach of security which, whether accidental or unlawful, results in the destruction, loss, alteration or unauthorised disclosure of, or unauthorised access to, the data (hereinafter referred to as a 'personal data breach'). When assessing the appropriate level of protection, the parties shall take

due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, and the risks to data subjects.

- 11.2. The Data Processor shall grant its staff access to the personal data being processed only to the extent strictly necessary for the performance, management and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have undertaken to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality.

12. Sensitive data

- 12.1. Where the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning a person's health, sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the processor shall apply specific restrictions and additional safeguards.

13. Documentation and compliance with the clauses

- 13.1. The parties must be able to demonstrate compliance with these clauses.
- 13.2. The processor shall deal promptly and appropriately with any requests from the controller regarding the processing of data in accordance with these clauses.
- 13.3. The processor shall provide the controller with all information necessary to demonstrate compliance with the obligations set out in these clauses and arising directly from Regulation (EU) 2016/679. At the request of the controller, the processor shall also allow for and contribute to an audit of the processing activities covered by these clauses at reasonable intervals or where there are indications of non-compliance. When deciding on an audit or inspection, the controller may take into account relevant certifications held by the processor.
- 13.4. The controller may carry out the audit itself or appoint an independent auditor. The audits may also include inspections at the processor's premises or physical facilities and shall, where appropriate, be carried out with reasonable notice.
- 13.5. The parties shall make the information referred to in this clause, including the results of audits, available to the competent supervisory authorities upon request.

14. Use of sub-processors

- 14.1. GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation to engage sub-processors listed in an agreed list. The processor shall expressly notify the

controller in writing, at least four weeks in advance, of any intended changes to this list involving the addition or replacement of sub-processors, thereby allowing the controller sufficient time to object to such changes before the sub-processor(s) in question are engaged. The processor shall provide the controller with the necessary information to enable the controller to exercise its right to object.

- 14.2. If the processor engages a sub-processor to carry out specific processing activities (on behalf of the controller), such engagement must be governed by a contract that imposes on the sub-processor essentially the same data protection obligations as those applicable to the processor under these clauses. The processor shall ensure that the sub-processor fulfils the obligations to which the processor is subject under these clauses and in accordance with Regulation (EU) 2016/679.
- 14.3. The processor shall provide the controller, upon request, with a copy of any such sub-processing agreement and any subsequent amendments thereto. To the extent necessary to protect trade secrets or other confidential information, including personal data, the processor may redact the text of the agreement before providing a copy.
- 14.4. The processor shall be fully liable to the controller for ensuring that the sub-processor fulfils its obligations under the contract concluded with the processor. The processor shall notify the controller if the sub-processor fails to fulfil its contractual obligations.
- 14.5. The processor shall agree a third-party beneficiary clause with the sub-processor, whereby the controller – in the event that the processor ceases to exist de facto or de jure or becomes insolvent – shall have the right to terminate the sub-processing agreement and instruct the sub-processor to erase or return the personal data.

15. International data transfers

- 15.1. Any transfer of data by the processor to a third country or an international organisation shall take place exclusively on the basis of documented instructions from the controller or in order to comply with a specific provision of Union law or the law of a Member State to which the processor is subject, and must be in accordance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- 15.2. The controller agrees that, in cases where the processor engages a sub-processor in accordance with clause 14 to carry out specific processing activities (on behalf of the controller) and such processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Data Processor and the sub-processor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for the application of these standard contractual clauses are met.

16. Assistance to the controller

- 16.1. The processor (contractor) shall inform the controller (client) without delay of any request from a data subject. A response shall only be provided if the processor has been authorised to do so by the client.
- 16.2. Taking into account the nature of the processing, the Contractor shall assist the Client in responding to requests from data subjects to exercise their rights and shall follow the Client's instructions in doing so.
- 16.3. Appropriate technical and organisational measures to assist the Client, as well as their scope and extent, are set out in Annex IV.
- 16.4. In addition, the Contractor shall assist the Client, taking into account the nature of the processing and the information available to it, in complying with the following obligations:
- a) Conducting a data protection impact assessment (DPIA) where processing is likely to result in a high risk to the rights and freedoms of natural persons.
 - b) Consulting the competent supervisory authority prior to processing if the DPIA indicates a high risk and no risk mitigation measures have been taken.
 - c) Ensuring the accuracy and up-to-date nature of personal data by immediately informing the Client if inaccurate or outdated data is identified.
 - d) Implementing the requirements of Article 32 of the GDPR (security of processing).
 - e) Immediately reporting personal data breaches to the client and providing all relevant information to enable the client to fulfil its information obligations towards data subjects (Articles 33 and 34 of the GDPR).
 - f) Providing support in the context of prior consultations with the supervisory authority (Article 36 of the GDPR).

17. Rights and obligations of the Contractor

- 17.1. Fulfilment of all legal obligations in accordance with Articles 28–33 of the GDPR.
- 17.2. Maintenance of confidentiality in accordance with Article 28(3)(b), Article 29 and Article 32(4) of the GDPR; use only of staff who have been appropriately instructed and trained.
- 17.3. Processing of personal data exclusively in accordance with the Client's instructions, provided there is no legal obligation to process it otherwise.
- 17.4. Implementation of and compliance with all necessary technical and organisational measures in accordance with Article 28(3)(c) and Article 32 of the GDPR (see Annex IV for details).
- 17.5. Cooperation with the supervisory authority upon request.

- 17.6. Regular monitoring of internal processes and technical and organisational measures to ensure processing in compliance with data protection regulations and the protection of data subjects' rights.
- 17.7. Provision of evidence of the measures taken to the client in accordance with Clause 16 of this contract and fulfilment of the obligations under Clause 21.

18. Notification of personal data breaches

- 18.1. In the event of a personal data breach, the processor shall cooperate with the controller and provide appropriate assistance to enable the controller to fulfil its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or, where applicable, Articles 34 and 35 of Regulation (EU) 2018/1725, taking into account the nature of the processing and the information available to the processor.

19. Breach of the security of data processed by the controller

- 19.1. In the event of a personal data breach relating to the data processed by the controller, the processor shall assist the controller as follows:
- 19.2. In promptly notifying the competent supervisory authority or authorities of the personal data breach after the controller becomes aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- 19.3. In obtaining the following information, which must be included in the controller's notification in accordance with Article 33(3) of Regulation (EU) 2016/679, whereby this information must include at least the following:
- a) The nature of the personal data, where possible, specifying the categories and the approximate number of data subjects concerned, as well as the categories and the approximate number of personal data records concerned;
 - b) the likely consequences of the personal data breach;
 - c) the measures taken or proposed by the controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects. If and insofar as not all of this information can be provided at the same time, the initial notification shall contain the information available at that time, and further information shall be provided without undue delay as soon as it becomes available;
- 19.4. In complying with the obligation under Article 34 of Regulation (EU) 2016/679 to notify the data subject without undue delay of the personal data breach, where the breach is likely to result in a high risk to the rights and freedoms of natural persons.

20. Breach of the protection of data processed by the processor

- 20.1. In the event of a personal data breach relating to the data processed by the processor, the processor shall notify the controller without undue delay after becoming aware of the breach. This notification must contain at least the following information:
- 20.2. A description of the nature of the breach (including, where possible, the categories and approximate number of data subjects concerned and the approximate number of data records concerned);
- 20.3. Contact details of a point of contact from whom further information regarding the personal data breach may be obtained;
- 20.4. The likely consequences and the measures taken or proposed to address the personal data breach, including measures to mitigate its possible adverse effects.
- 20.5. If and to the extent that not all of this information can be provided at the same time, the initial notification shall contain the information available at that time, and further information shall be provided without undue delay as soon as it becomes available. The parties shall set out in Annex IV all other information that the processor must provide in order to assist the controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

21. Subcontracting

With regard to the engagement of subcontractors, the parties agree as follows:

- The Contractor may only enter into subcontracting arrangements relating to the processing of personal data covered by this contract with the prior written consent of the Client (in accordance with Article 28(2), first sentence, of the GDPR).
- The Client grants the Contractor general authorisation to engage sub-processors. The processor shall inform the Client of any intended change regarding the engagement or replacement of other processors, thereby giving the Client the opportunity to object to such changes (in accordance with Article 28(2), second sentence, of the GDPR).

- 21.1. The transfer of the Client's personal data to the sub-processor and the sub-processor's first performance of its duties shall only be permitted once all conditions for sub-processing have been met.
- 21.2. The Contractor shall impose on the sub-processor, in writing, the same obligations as those to which the Contractor itself is subject under this contract vis-à-vis the Client.
- 21.3. If the sub-processor fails to fulfil its data protection obligations, the Contractor shall be liable to the Client for the sub-processor's compliance with its obligations in accordance with Article 28(4) of the GDPR.
- 21.4. Prior to engaging a sub-processor, the Contractor shall satisfy itself that the sub-processor has implemented the necessary technical and organisational measures.

21.5. Where sub-processors in third countries are to be engaged, the Contractor shall ensure that an adequate level of data protection within the meaning of Articles 44 et seq. of the GDPR is guaranteed by the respective sub-processor. The sub-processor must appoint a representative in the EU.

21.6. The Client hereby consents to the establishment of sub-processing relationships in accordance with Annex III Sub-processors.

22. The Client's rights of supervision

22.1. The Contractor shall ensure that the Client is able to verify the Contractor's compliance with its obligations under Article 28 of the GDPR.

22.2. In the course of such verification, the Contractor shall provide all necessary information and details, submit relevant documents and, in particular, demonstrate the implementation of technical and organisational measures. Evidence of such measures, which do not relate solely to the specific contract, may be provided by:

22.3. Compliance with approved codes of conduct, in accordance with Article 40 of the GDPR

- a) certification in accordance with an approved certification procedure pursuant to Article 42 of the GDPR
- b) current certificates, reports or extracts from reports issued by independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors)
- c) appropriate certification through an IT security or data protection audit (e.g. in accordance with BSI Basic Protection).

22.4. Following timely consultation, the Client may, during normal business hours, inspect the Contractor's technical and organisational measures for compliance with this Agreement or have them inspected by a competent third party, provided that such third party is not in competition with the Contractor.

22.5. The Client shall carry out checks only to the extent necessary and shall not unduly disrupt the Contractor's business operations in doing so.

23. Deletion and return of personal data

23.1. Upon completion of the contractually agreed work or earlier upon request by the Client – at the latest upon termination of the service agreement – the Contractor shall hand over to the Client all documents that have come into its possession, all processing and usage results produced, and all data sets relating to the contractual relationship, or, subject to prior consent, destroy them in accordance with data protection regulations. The same applies to test and scrap material.

23.2. The deletion log must be provided upon request. Statutory retention obligations remain unaffected.

24. Legal liability

24.1. The statutory liability provisions pursuant to Article 82 of the GDPR apply. Any limitations of liability between the parties (e.g. arising from the main contract) shall not apply in this regard.

25. Final provisions

25.1. This agreement is governed by German law.

25.2. Should any provision of this contract be or become invalid, this shall not affect the validity of the remaining provisions. In such a case, the contracting parties shall endeavour to find a solution that corresponds to the current intent in terms of its economic effect. This shall also apply if a gap requiring supplementation becomes apparent during the performance of the contract.

25.3. Amendments and additions to this contract must be made in writing. This shall also apply to the waiver of the written form requirement.

25.4. The annexes to this contract are:

Annex I:	Type of data and categories of data subjects
Annex II:	List of parties
Annex III:	Sub-processors
Annex IV:	Technical and organisational measures of the processor

26. Breaches of the clauses and termination of the contract

26.1. If the processor fails to fulfil its obligations under these clauses, the controller may – without prejudice to the provisions of Regulation (EU) 2016/679 – instruct the processor to suspend the processing of personal data until it complies with these clauses or the contract is terminated. The processor shall inform the controller without delay if, for whatever reason, it is unable to comply with these clauses.

26.2. The controller shall be entitled to terminate the contract insofar as it relates to the processing of personal data in accordance with these clauses if

26.3. I. the controller has suspended the processing of personal data by the processor in accordance with point (a) and compliance with these clauses has not been restored within a reasonable period, but in any event within one month of the suspension;

26.4. II. the processor breaches these clauses to a significant extent or on a persistent basis, or fails to fulfil its obligations under Regulation (EU) 2016/679;

26.5. III. the processor fails to comply with a binding decision of a competent court or the competent supervisory authorities concerning its obligations under these clauses or Regulation (EU) 2016/679.

- 26.6. The processor shall be entitled to terminate the contract insofar as it relates to the processing of personal data in accordance with these clauses if the controller insists on the fulfilment of its instructions after having been informed by the processor that its instructions breach applicable legal requirements in accordance with clause 10.2.
- 26.7. Upon termination of the contract, the processor shall, at the controller's discretion, either delete all personal data processed on the controller's behalf and certify to the controller that this has been done, or return all personal data to the controller and delete existing copies, unless there is an obligation under Union law or the law of the Member States to retain the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these clauses.

Appendix I: Type of data and categories of data subjects

Type of data

The following types of data are covered by this contract (*please tick the relevant boxes*):

- Personal details (e.g. name, address)
- Communication data (e.g. telephone, email)
- Age
- Special categories of personal data pursuant to Article 9(1) of the GDPR (e.g. health data)
- Applicant data
- Contract/employee master data (e.g. personnel and identification number)
- Wage and salary data
- Tax/accounting data
- Working time data
- Employee appraisals
- Employee qualifications and characteristics
- Telecommunications billing data
- Telecommunications connection data
- Planning and control data
- Contract billing and payment data
- Customer history
- Customer behaviour data
- User IDs
- Passwords
- Access data
- Bank account details
- Credit card details
- Audio data
- Image data
- Video data
- Credit reference information (credit agencies; public registers, etc.)
- Other, namely machine data, therapy data

Categories of data subjects

The following groups of data subjects are covered by this mandate:

- Employees
- Trainees and interns
- Job applicants
- Former employees
- Freelancers
- Shareholders
- Relatives of employees
- Customers
- Prospective customers
- Suppliers and service providers
- Tenants
- Business partners
- Consultants

- Visitors
- Members of the press
- Subscribers
- Commercial agents
- Contact persons
- Others, namely patients

*Description of the processing**Categories of data subjects whose personal data is processed*

X Customers X Patients

Categories of personal data processed

X Name

X Email address

X IP address

X Device information

X Gender

Sensitive data processed (if applicable) and restrictions or safeguards applied that fully take into account the nature of the data and the associated risks, e.g. strict purpose limitation, access restrictions (including access only for staff who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures

X Data, results and records from training sessions

X Data, results and records from performance evaluations

Type of processing

Collection and storage of data

Purpose(s) for which the personal data is processed on behalf of the controller

Creation of personalised training plans tailored to patients' individual performance and progress.

Duration of processing

In accordance with the term of the main contract.

Where processing is carried out by (sub)processors, the subject matter, nature and duration of the processing must also be specified.

Provision of the SaaS software for the processing of data for the purposes set out above for the duration of the main contract.

Appendix II: List of parties

Responsible party:

As per the quotation/order confirmation/invoice for the THERA-Trainer senso product and the associated software.

Data processor(s): *[Name and contact details of the data processor(s) and, where applicable, the data protection officer of the data processor]*

Name: medica Medizintechnik GmbH

Address: Blumenweg 8, 88454 Hochdorf

Name, role and contact details of the contact person:

Dr. Jonathan Kopf
CEO


Dr, Jonathan Kopf, CEO

Appendix III: Subcontractors

The Client agrees to the Contractor engaging the following subcontractors:

Company name / Subcontractor's company name	Postal address	Other contact details (email, telephone)	Contact person	Subject of the subcontract
Dividat AG	Neuhofstrasse 3, CH 8834 Schindellegi	info@dividat.ch +41 44 586 88 34	Joris van het Reve	Provision of software applications (SaaS) in the field of care and health promotion
Company name / Subcontractor's company name	Postal address	Other contact details	Contact person	Subject of the subcontract
Company name / Subcontractor's company name	Postal address Postal address	Other contact details	Contact person	Subject of the subcontract
Company name / Subcontractor's company name	Post-adresse	Other contact details	Contact person	Subject of the subcontract

Appendix IV: Technical and organisational measures to be taken by the contractor

In accordance with this agreement, medica Medizintechnik GmbH has established appropriate security measures (technical and organisational measures) within the meaning of Article 32 of the GDPR. Given the sensitivity of the data processed by medica Medizintechnik GmbH, we wish to prevent these security measures from being freely accessible. The policy will be made available to the client (upon request) and can be requested at info@thera-trainer.de.

Contractually agreed notification obligations, e.g. in the event of changes, remain unaffected by this.