STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is 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).

b) 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.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2
Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3
Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5
Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6
Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7
Obligations of the Parties

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

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

7.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfil its contractual obligations.The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8
Assistance to the controller

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its

obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   I. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

   II. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

   III. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9
Notification of personal data breach

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

9.1 Data breach concerning data processed by the controller

a) In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

b) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become 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);

c) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679/

   I. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   II. the likely consequences of the personal data breach;

   III. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

d) Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it

becomes available, subsequently be provided without undue delay.

e) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III

FINAL PROVISIONS

Clause 10
Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

I. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

II. the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

III. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I
LIST OF PARTIES

Controller(s):
As per offer/order confirmation/invoice for the product THERA-Trainer senso and the associated software.

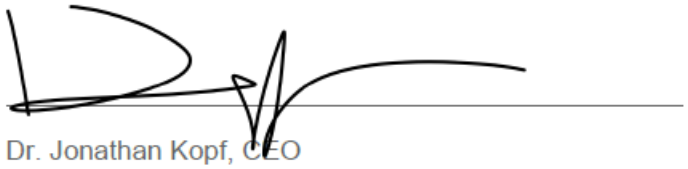
Processor(s): [Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]

Name: medica Medizintechnik GmbH

Contact details: Blumenweg 8 88454 Hochdorf (Germany)

Name and position of signing person:

Dr. Jonathan Kopf
CEO



ANNEX II
DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data are processed
☒ Customers ☒ Patients

Categories of personal data processed
☒ Name
☒ E-mail address
☒ IP address
☒ Device information
☒ Gender

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

☒ data, results and records of training sessions
☒ Data, results and records of performance evaluations.

Type of processing
Collection and storage of data

Purpose(s) for which the personal data are processed on behalf of the data controller
To create personalised training plans based on individual patient performance and progress.

Duration of the processing
As per duration from main contract

In the case of processing by (sub)processors, the subject, nature and duration of the processing shall also be indicated.

Provision of the SaaS software to process the data relating to the above for the duration of the main contract.

ANNEX III

TECHNICAL AND ORGANISATIONAL MEASURES WITHIN THE MEANING OF ARTICLE 32 (1) DSGVO INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

medica Medizintechnik GmbH

Data protection concept

Technical and organizational measures within the meaning of Art. 32 (1) DSGVO

Booth:
June 2018

Author:
Stefan Fischerkeller - German Data Protection Law Firm

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

Data protection concept

Technical and organizational measures within the meaning of Article 32 (1)

Form	Status 28.06.2018	Classification:	Responsible:	Version 1.1

Table of contents

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

Data protection concept

Technical and organizational measures within the meaning of Article 32 (1)

Form	Status 28.06.2018	Classification:	Responsible:	Version 1.1

1 Introduction

The EU General Data Protection Regulation (GDPR) contains specifications on how personal data should be handled in technical and organizational terms. This serves the goal of data security. Data security thus represents a further and complementary aspect of data protection.

Data security is regulated by law in Art. 32 (1) DSGVO. These regulations require that such technical and organizational measures be taken as are necessary to ensure the protection of personal data.

The law mentions various areas of control, each of which still contains various sub-items:

(1) Confidentiality

(2) Integrity

(3) Availability and resilience

(4) Procedures for regular review, assessment and evaluation

(5) Pseudonymization and encryption

We present these measures below in order to comply with our information obligations under Art. 28 (3) lit.
c) GDPR.

2 Organizational

medica Medizintechnik GmbH ensures the written documentation of the current data protection level, as well as the written work instructions, guidelines and leaflets for employees. The employees involved in data processing are bound to data secrecy or confidentiality according to Art. 28 para. 3 p. 2 lit. B, 29, 32 para. 4 DSGVO.

Some safeguards in the following checklist pertaining to this area are not separately identified because they are the responsibility of the subcontractors or are not published in detail for reasons of maintaining security through confidentiality.

3 Safeguarding measures

The following points describe the technical and organizational measures operated by medica Medizintechnik GmbH:

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

3.1 Confidentiality (Art. 32 para. 1 lit. b DSGVO)

3.1.1 Access control

Access control comprises measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

- Gatekeeper/Personnel Control
- Central department is occupied
- Only persons with authorization card can visit the building (outside theoccupation hours of the central department) enter
- The administration and maintenance of the mechanical access control systems is regulated and documented
- The distribution rooms or areas (building services) are secured against unauthorized access
- Rooms are locked; associated keys only available to authorized persons
- Use of anti-burglary measures (alarm system with remote connection to a security service)
- Enterprise servers are operated in a locked and access-secured room. Only authorized persons have access to the server room
- The network components are located in designated access-controlled rooms (access-secured by locked server cabinets or locked rooms)

3.1.2 Access control

Measures suitable for preventing data processing systems from being used by unauthorized persons.

- It is ensured via the rights management or, if individually required (in monitoring with IT), that users are only granted access to the network services they are expressly authorized to use
- Only authorized persons have logical access to the network components
- The (remote) maintenance process is monitored. The monitoring takes place via a log of the firewall
- Connection establishment to the network from outside via SSTP encryption

In addition, the following measures are used:

- Assignment of user profiles to IT systems
- Use of VPN technology
- Security locks
- Authentication with username and password
- Smartphone content encryption
- Use of anti-virus software
- Binding procedure for the assignment of rights
- Disconnection of superfluous services
- Network monitoring with alerting

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- Hardware firewall deployment
- Functional restriction of the use of client systems and screen workstations (restrictive assignment of rights)

3.1.3 Access control

Measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

The restriction of access is ensured by:

- Disk management
- Software-based exclusion (authorization concept)
- Restriction of user access
- Restrictive access authorization/project-related accesses
- Drive usage/allocation concept
- Authorization allocation procedure
- Graduated access rights with logging/logging
- IT security guidelines/policies
- Personal data is generally not stored on external data carriers
- There is an instruction on how to deal with data carriers that are no longer needed (this also includes written or printed paper)
  - Data protection and data security work instruction
  - Sub-process description of all processes in IT
- There is an instruction on how to proceed with the disposal or further use of devices that are equipped with storage media
  - Sub-process description of all processes in IT

3.1.4 Separation requirement

Measures to ensure that data collected for different purposes can be processed separately.

- Personal data on the systems are physically separated from each other (processing of different data sets on separate systems)
- On the systems, personal data are logically separated from each other (different data records in a uniform database are marked according to their purpose (software-based distinguishability)
- There is a corresponding authorization concept

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- Database rights exist
- Multi-client capability is implemented across the board for the processes affected by it
- Office, development, test and effective systems or test and productive data are located on different servers and in the same network
- It is ensured that only test data is processed in the development and test system

3.2 Integrity (Art. 32 para. 1 lit. b DSGVO)

3.2.1 Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and determine to which entities personal data is intended to be transmitted by data transmission equipment.

- All persons (including new employees) involved in the processing/use of personal data are obliged to maintain confidentiality
  - Data protection work instruction
  - Privacy Commitment Statement for Administrators
  - Company agreement
- In particular, information on data protection is handed out to new employees and countersigned by them (as part of the work instruction).
- Employees who process/use personal data are trained in data protection-compliant behavior at the workplace through data protection training - awareness measures.
- Application of the regulations for the on-boarding/off-boarding process
- Security measures such as VPN and encryption are implemented for the physical transport of data media

Additional measures are used:

- Establishment of transport connection only between defined systems secured by certificates
- VPN access for mobile workstations/home offices
- Controlled destruction of data carriers and paper documents according to DIN 66399

3.2.2 Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- In a folder with version management it is documented which user or procedure-related evaluation options are used in our company (in time recording it is 30 days)

- It is possible to check retrospectively whether data is being processed and by whom:

  - User profiles
  - Authorization concepts
  - Logging of the entry, modification and deletion of data
  - Firewall logging (TCP/IP)
  - Logging via Active Directory

Availability and resilience (Art. 32(1)(b) and (c) GDPR)

Measures to ensure that personal data is protected against accidental destruction or loss and can be quickly recovered in the event of a physical or technical incident.

Accidental destruction/loss of personal data is prevented by adequate measures:

- Deployment uninterruptible power supply incl. overvoltage protection and emergency generator
- Extinguishing system/fire/smoke detection system
- Lightning protection equipment
- Use of air-conditioning system incl. documentation of air-conditioning technology
- Distribution of network components to several protected areas for the purpose of risk/failure minimization
- Monitoring room temperature/humidity etc.
- Overvoltage protection
- Alarm system incl. forwarding to control center, plant security, fire department, guard service, etc.
- A risk and vulnerability analysis is performed and assessed by IT. The risk factors against maintaining DP operations are examined in the process.
- It exists a backup/recovery concept and a backup data center. The requirements for the backup are documented in this concept
- There is an emergency manual, which is continuously updated
- For the DV startup there is a written document
- There is a security archive in the private living quarters of the shareholder/managing director, Mr. Otto Höbel, with a restrictive access authorization concept.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

3.3 Procedures for regular review, assessment and evaluation (Art. 25 (1) GDPR; Art. 32 (1) (d) GDPR)

3.3.1 Data protection management

medica Medizintechnik GmbH is managed by the German Data Protection Office (external data protection officer is Mr. Stefan Fischerkeller). The German Data Protection Office uses a specially created data protection management system (DSMS), in which all measures, procedures and activities in the area of data protection are mapped. The DSMS contains the most important data protection requirements and a comprehensive structure for mapping data protection measures and also includes an action plan for legally compliant implementation of the EU General Data Protection Regulation (accountability pursuant to Article 5 (2) DSGVO).

3.3.2 Incident Response Management

A proceduralized handling of security incidents has been implemented. In the event of an incident, employees inform IT or their supervisor immediately. This is followed by coordination with the data protection officer. The processing by the data protection officer is ensured by appropriate deputization arrangements.

3.3.3 Privacy-friendly default settings (Art. 25 (2) GDPR)

In principle, only data that is appropriate and necessary for business purposes is collected and processed. Automated data collection and processing procedures are designed in such a way that only the necessary data can be collected. The data of the customers are partly kept in encrypted form.

3.3.4 Order control

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Employees who have access to the systems as administrators have all been instructed with regard to data protection, are bound to data secrecy, and have accepted corresponding confidentiality and non-disclosure agreements as part of their employment contract.

If medica Medizintechnik GmbH uses subcontractors for data processing, certain requirements will be implemented. This includes ensuring the technical-organizational measures of the subcontractors within the meaning of Art. 28 DSGVO in conjunction with Art. 32 para. 1 DSGVO.

Requirements for entering into a subcontracting relationship:

- Contract for commissioned data processing in accordance with the requirements of Art. 28 (3) DSGVO.
- German service providers have appointed a company data protection officer and ensure through the data protection organization that he or she is appropriately and effectively integrated into the relevant operational processes.
- Description Checks and Audits.
- Placement of individual orders. Confirmation of oral orders.

THERA-Trainer by medica Medizintechnik GmbH
Blumenweg 8 | 88454 Hochdorf
Tel +49 7355-93 14-0 | info@thera-trainer.com | www.thera-trainer.com

- A contract template for commissioned data processing is available for the transfer of personal data to external service providers, which contains corresponding regulations for control.

3.4 Pseudonymization and encryption (Art. 32 para. 1 lit. a DSGVO)

If a direct reference to a person is not necessary, the possibility of pseudonymization is used if this is possible and the effort is in a reasonable proportion to the intended protective purpose (data economy). The data transfer from the website takes place via SSL encryption.

3.5 Cooperation with the German Data Protection Office

In order to comply with the data protection requirements according to the applicable EU General Data Protection Regulation, medica Medizintechnik GmbH cooperates with the German Data Protection Law Firm. In addition to the creation of guidelines and aids to action, the German data protection law firm advises medica Medizintechnik GmbH on all issues relating to data protection and provides Mr. Stefan Fischerkeller as the company's external data protection officer in accordance with Art. 37 DSGVO.

Contact persons of the German Data Protection Office are:

Stefan Fischerkeller

Diplomverwaltungswirt (FH), certified expert data protection officer (DESAG) E-mail:

fischerkeller@ddsk.de

Tel.: 07544 / 904 96 91

Maximilian Musch

Magister Artium, certified expert data protection officer (udis) E-mail:

musch@ddsk.de

Tel.: 07544 / 904 96 92

German data protection law firm

Lake Constance office

Richard-Wagner-Strasse 2, 88094

Oberteuringen www.deutsche-

datenschutzkanzlei.de

DEUTSCHE DATENSCHUTZ KANZLEI

ANNEX IV
LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Sub-processor	Country	Contact details	Short description of the service
Dividat AG	Switzerland	Neuhofstrasse 3, 8834 Schindellegi	Provision of software applications (SaaS) in the field of care and health promotion.