Data Processing Agreement (DPA) including Standard Contractual Clauses (SCC) (Art. 28, 29 DSGVO)

- *state: 15.08.2025* -

Preamble:

This data processing agreement governs the rights and obligations of the contracting parties in connection with the processing of personal data on behalf of the other party in accordance with Art. 28 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 part of this agreement and have been supplemented in accordance with the requirements of the European Commission by specific, contractually necessary additions – in particular by information on the technical and organisational measures, the type of data processed, the purposes of the processing and the parties and sub-processors involved.

This contract applies to all processing activities in connection with the service contract concluded between the parties in which employees of the contractor or subcontractors commissioned by the contractor process personal data (‘data’) of the client on behalf of the contractor.

The terms used in this contract are to be understood in accordance with the definitions of the EU General Data Protection Regulation (‘GDPR’).

1. Purpose and scope

1.1. These standard contractual clauses (hereinafter referred to as ‘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 the clauses.

1.5. These clauses are 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. Irrevocability of the clauses

2.1. The parties undertake not to amend the clauses, except to supplement or update the information specified in the annexes

2.2. This does not prevent the parties from incorporating the standard contractual clauses set out in these clauses into a more comprehensive contract and adding further clauses or additional guarantees, provided that these do not directly or indirectly contradict the clauses or restrict the fundamental rights or freedoms of the persons concerned.

3. Dimensioning

3.1. Where terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 are used in these clauses, those 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 shall 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 the data subjects.

4. Priority

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

5. Tying clause

5.1. An organisation that is not a party to these clauses may join them at any time as a controller or processor with the consent of all parties by completing the appendices and signing Annex I.

5.2. Upon completing and signing the appendices referred to in clause 51, the acceding organisation shall be treated as a party to these clauses and shall have the rights and obligations of a controller or processor as specified in Appendix II.

5.3. The acceding organisation shall not have any rights or obligations under these clauses 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: Therapy data processing

6.2. The processor shall process the personal data only for the specific purposes specified in Annex I, unless it receives further instructions from the controller.

6.3. The contractor shall process personal data for the client within the meaning of Art. 4 No. 2 and Art. 28 GDPR.

6.4. The data shall only be processed by the processor for the period specified in Annex I.

6.5. Subject to the provisions of any main contract that may exist, any termination must be made in writing.

7. Processing framework / Type and purpose of processing

7.1. The contractor processes personal data as follows and for the following purpose:

a) Storage and visualisation of device-specific and device-independent therapy data assigned to a user (patient)

7.2. Type of personal data and categories of data subjects

a) The type of data and categories of data subjects covered by this agreement are defined in Appendix I: Type of 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 commencing processing, in particular with regard to the specific execution of the contract, and 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 adjustment, this shall be implemented by mutual agreement.

8.2. The contractor must establish and ensure security in accordance with Art. 28(3)(c) and Art. 32 GDPR, in particular in conjunction with Art. 5(1) and (2) GDPR. Overall, the technical and organisational measures to be taken are measures for data security and for ensuring a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In doing so, the state of the art, the implementation costs 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 Art. 32(1) GDPR, must be taken into account.

8.3. The details of the contractor's technical and organizational measures (TOMs) are set out in Appendix IV.

8.4. The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. However, the security level of the specified measures must not be compromised. Significant changes must be documented.

9. Place of processing

9.1. The data is processed 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 Art. 44 et seq. GDPR are met.

10. Instructions and authority to issue instructions to the contractor

10.1. The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union law or the law of a Member State to which the processor is subject. In such a case, the processor shall inform the controller of those legal requirements before processing, unless prohibited by that law on grounds of important public interest. The controller may give further instructions during the entire processing of personal data. These instructions shall always be documented.

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

11. Security of processing

11.1. The processor shall implement at least the technical and organizational measures listed in Annex IV to ensure the security of personal data. This includes protecting the data against any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the data (hereinafter referred to as “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 the data subjects.

11.2. The processor shall only grant its personnel access to the personal data that is the subject of the processing to the extent that this is strictly necessary for the performance, management, and monitoring of the contract. The processor shall ensure that the persons authorized to process the personal data received have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

12. Sensitive data

12.1. If the processing involves 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 concerning criminal convictions and offenses (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.

13.3. The processor shall promptly and appropriately respond to requests from the controller regarding the processing of data in accordance with these clauses.

13.4. The processor shall provide the controller with all information necessary to demonstrate compliance with the obligations laid down in these clauses and arising directly from Regulation (EU) 2016/679. At the request of the controller, the processor shall also allow and contribute to the audit of the processing activities covered by these clauses at reasonable intervals or in the event of indications of non-compliance. When deciding on an audit or inspection, the controller may take into account relevant certifications of the processor.

13.5. The controller may conduct the audit itself or appoint an independent auditor. Audits may also include inspections of the processor's premises or physical facilities and shall be conducted with reasonable advance notice, where appropriate.

13.6. The parties shall provide the competent supervisory authorities with the information referred to in this clause, including the results of audits, upon request.

14. Use of subcontractors

14.1. GENERAL WRITTEN PERMISSION: The processor has the general authorization of the controller to engage subprocessors listed in an agreed list. The processor shall notify the controller in writing at least four weeks in advance of any intended changes to this list by adding or replacing subprocessors, thereby allowing the controller sufficient time to raise objections to these changes before the relevant subprocessor(s) is/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), this engagement must be by way of a contract that imposes substantially the same data protection obligations on the sub-processor as those applicable to the processor under these clauses. The processor shall ensure that the sub-processor fulfills 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 with a copy of any such subcontracting agreement and any subsequent amendments thereto upon request. Where 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 the subprocessor's compliance with its obligations under the contract concluded with the processor. The processor shall notify the controller if the subprocessor fails to comply with its contractual obligations.

14.5. The processor shall agree with the subprocessor on a third-party beneficiary clause whereby the controller shall have the right, in the event that the processor ceases to exist de facto or de jure or becomes insolvent, to terminate the subcontract and instruct the subprocessor to delete or return the personal data.

15. International data transfers

15.1. Any transfer of data by the processor to a third country or international organization shall be carried out exclusively on the basis of documented instructions from the controller or in order to comply with a specific provision under 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 certain processing activities (on behalf of the controller) and these 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 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. Support for the controller

16.1. The processor (contractor) shall inform the controller (client) immediately of any request from a data subject. A response shall only be provided if the processor has been authorized to do so by the client.

16.2. Taking into account the nature of the processing, the contractor shall support 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 organizational measures to support the client, as well as their scope and extent, are specified in Annex IV.

16.4. In addition, the contractor shall support the client in complying with the following obligations, taking into account the nature of the processing and the information available to it:

a) Conducting a data protection impact assessment (DPIA) if 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 reveals a high risk and no measures have been taken to mitigate the risk.

c) Ensuring the accuracy and timeliness of personal data by immediately informing the client if inaccurate or outdated data is found.

d) Implementing the requirements of Art. 32 GDPR (security of processing).

e) Immediately reporting personal data breaches to the client and providing all relevant information to fulfill its information obligations to data subjects (Articles 33 and 34 GDPR).

f) Providing support in the context of prior consultations with the supervisory authority (Article 36 GDPR).

17. Rights and obligations of the client

17.1. Fulfillment of all legal obligations in accordance with Articles 28–33 GDPR.

17.2. Maintenance of confidentiality in accordance with Articles 28(3)(2)(b), 29, and 32(4) GDPR, use only by obligated and trained employees.

17.3. Processing of personal data exclusively in accordance with the client's instructions, unless there is a legal obligation to process it otherwise.

17.4. Implementation of and compliance with all necessary technical and organizational measures in accordance with Art. 28 (3) sentence 2 lit. c), 32 GDPR (for details, see Annex IV).

17.5. Cooperation with the supervisory authority upon request.

17.6. Regular monitoring of internal processes and technical and organizational measures to ensure data protection-compliant processing and the protection of the rights of data subjects.

17.7. Proof of the measures taken to the client in accordance with Section 16 of this contract and fulfillment of the obligations under Section 21.

18. Reporting violations of personal data protection

18.1. In the event of a personal data breach, the processor shall cooperate with and assist the controller so that the controller can fulfill 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 protection of data processed by the controller

19.1. In the event of a breach of the protection of personal data in connection with the data processed by the controller, the processor shall support the controller as follows:

19.2. by promptly notifying the competent supervisory authority or authorities of the personal data breach after the controller becomes aware of the breach, where relevant (unless the personal data breach is unlikely to result in a risk to the personal rights and freedoms of natural persons);

19.3. in obtaining the following information, which must be included in the controller's notification pursuant to Article 33(3) of Regulation (EU) 2016/679, whereby this information must include at least the following:

a) the nature of the personal data, as far as possible, specifying the categories and approximate number of data subjects concerned and the categories and 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 to the extent that not all this information can be provided at the same time, the initial communication 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 compliance 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 that 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 breach of personal data protection in connection with the data processed by the processor, the processor shall notify the controller without delay after becoming aware of the breach. This notification shall include at least the following information:

20.2. a description of the nature of the breach (if possible, specifying the categories and approximate number of data subjects and the approximate number of data records affected);

20.3. contact details of a point of contact where further information about the personal data breach can 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 notice 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 specify 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 commissioning of subcontractors, the parties agree as follows:

☐ The contractor may only establish subcontracting relationships with regard to the contractual processing of personal data with the prior written consent of the client (in accordance with Art. 28 (2) sentence 1 GDPR).

☒ The client grants the contractor general approval to use subcontractors. The processor shall inform the client of any intended change in relation to the involvement or replacement of other processors, thereby giving the client the opportunity to object to such changes (in accordance with Art. 28 (2) sentence 2 GDPR).

21.1. The transfer of the client's personal data to the subcontractor and the subcontractor's initial activities are only permitted once all the requirements for subcontracting have been met.

21.2. The contractor must oblige the subcontractor in writing to the same extent as it is itself obliged to the client under this contract.

21.3. If the subcontractor fails to comply with its data protection obligations, the contractor shall be liable to the client for compliance with the obligations of that subcontractor in accordance with Art. 28 (4) GDPR.

21.4. Before commissioning the subcontractor, the contractor shall satisfy itself that the subcontractor has taken the necessary technical and organizational measures.

21.5. If subcontractors in third countries are to be involved, the contractor shall ensure that the respective subcontractor guarantees an adequate level of data protection within the meaning of Art. 44 et seq. GDPR. The subcontractor shall appoint a representative in the EU.

21.6. The client hereby agrees to the establishment of subcontracting relationships in accordance with Appendix III Subcontractors.

22. Kontrollrechte des Auftraggebers

22.1. The contractor shall ensure that the client can verify compliance with the contractor's obligations under Art. 28 GDPR.

22.2. As part of the audit, the contractor shall provide all necessary information and details, submit documents, and, in particular, provide evidence of the implementation of technical and organizational measures. Proof of such measures, which do not only relate to the specific order, can be provided by:

22.3. Compliance with approved rules of conduct, in accordance with Art. 40 GDPR

a) Certification in accordance with an approved certification procedure in accordance with Art. 42 GDPR

b) Current certificates, reports, or report excerpts from independent bodies (e.g., auditors, internal auditors, data protection officers, IT security departments, data protection auditors, quality auditors)

c) Appropriate certification by IT security or data protection audit (e.g., according to BSI basic protection).

22.4. After timely consultation, the client may, during normal business hours, review the contractor's technical and organizational measures for compliance with this agreement or have them reviewed by a competent third party, provided that the third party is not in a competitive relationship with the contractor.

22.5. The client shall only carry out checks to the extent necessary and shall not disproportionately 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 must hand over to the client all documents that have come into its possession, processing and usage results created, and data stocks related to the contractual relationship, or destroy them in accordance with data protection regulations after prior consent. The same applies to test and reject material.

23.2 The deletion log must be presented upon request. The statutory retention obligations remain unaffected.

24. Legal liability

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

25. Final provisions

25.1. German law applies to this agreement.

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

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

25.4. The following are annexes to this contract:

Annex I: Type of data and categories of data subjects

Annex II: List of parties

Annex III: Subcontractors

Annex IV: Technical and organizational measures taken by the contractor

26. Verstöße gegen die Klauseln und Beendigung des Vertrags

26.1. If the processor fails to comply with 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 concerns the processing of personal data under these clauses if

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

26.4. II. the processor is in material breach of these clauses or fails to comply with its obligations under Regulation (EU) 2016/679 on a persistent basis;

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 and Regulation (EU) 2016/679

26.6. The processor is entitled to terminate the contract insofar as it concerns the processing of personal data in accordance with these clauses if the controller insists on fulfilling its instructions after being informed by the processor that its instructions violate applicable legal requirements in accordance with Section 10.2.

26.7. Upon termination of the contract, the processor shall, at the controller's discretion, either delete all personal data processed on behalf of the controller 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 to store the personal data under Union or Member State law. 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 order (please tick the applicable boxes):

☒ Personal master data (e.g., name, address)

☐ Communication data (e.g., telephone, email)

☐ Age

☒ Special categories of personal data pursuant to Art. 9 (1) 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 evaluations

☐ Employee qualifications and characteristics

☐ Telecommunications billing data

☐ Telecommunications connection data

☒ Planning and control data

☐ Contract billing and payment data

☐ Customer history

☐ Customer behavior data

☐ User IDs

☒ Passwords

☒ Access data

☐ Bank account details

☐ Credit card details

☐ Audio data

☐ Image data

☐ Video data

☐ Information (credit agencies; public directories, etc.)

☒ Other, namely machine data, therapy data

Categories of data subjects

The following groups of data subjects are covered by the contract:

☒ Employees

☐ Trainees and interns

☐ Applicants

☐ Former employees

☐ Freelancers

☐ Shareholders

☐ Relatives of employees

☐ Customers

☐ Prospective customers

☐ Suppliers and service providers

☐ Tenants

☐ Business partners

☐ Consultants

☐ Visitors

☐ Representatives of the press

☐ Subscribers

☐ Sales representatives

☐ Contact persons

☒ Others, namely patients

Description of processing

Categories of data subjects whose personal data is processed

☒ Customers ☒ Patients

Categories of personal data that is processed

☒ Name

☒ Email address

☒ IP address

☒ Device information

☒ Gender

Sensitive data processed (if applicable) and restrictions or safeguards applied that fully reflect the nature of the data and the risks involved, e.g., strict purpose limitation, access restrictions (including access *only for employees who have undergone special training), records of access to the data, restrictions on onward transfers, or additional security measures*

☒ Data, results, and records from training sessions

☒ 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 personalized training plans tailored to the individual performance and progress of patients.

Duration of processing

In accordance with the term of the main contract.

In the case of processing by (sub)processors, the subject matter, type, and duration of the processing must also be specified.

Provision of the SaaS software for processing the data for the above-mentioned purposes for the duration of the main contract.

Appendix II: List of parties

Responsible party(ies):

In accordance with the offer/order confirmation/invoice for the THERA-Trainer senso product and the associated software.

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

Name: medica Medizintechnik GmbH

Address: Blumenweg 8, 88454 Hochdorf, Germany

Name, position, and contact details of the contact person:

Dr. Jonathan Kopf
CEO

Dr, Jonathan Kopf, CEO

Appendix III: Subcontractors

The client agrees to the contractor commissioning the following subcontractors:

Company Name / Subcontractor Company	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 nursing and health promotion

APPENDIX IV: TECHNICAL AND ORGANIZATIONAL MEASURES TAKEN BY THE CONTRACTOR

Description

Technical and organizational pursuant to the meaning of Art. 32(1) GDPR

Form	State: 19.12.2023	Classification: **confidential**	Resp.: DSB	Version 2.1

medica Medizintechnik GmbH
Blumenweg 8
88454 Hochdorf

Technical and organizational pursuant to the meaning of Art. 32(1) GDPR

Stand: December 2023

Author: DSB

Table of Contents

TABLE OF CONTENTS 2

1 INTRODUCTION 3

2 ORGANIZATIONAL MATTERS 4

3 DATA PROTECTION MANAGEMENT 4

4 PROTECTIVE MATTER ....FEHLER! TEXTMARKE NICHT DEFINIERT.

4.1 CONFIDENTIALITY (ART. 32(1)(B) GDPR) .... **FEHLER! TEXTMARKE NICHT DEFINIERT.**

4.1.1 Entry control .... **Fehler! Textmarke nicht definiert.**
4.1.2 Access control .... **Fehler! Textmarke nicht definiert.**
4.1.3 Control access .... **Fehler! Textmarke nicht definiert.**
4.1.4 Separation requirement .... **Fehler! Textmarke nicht definiert.**

4.2 INTEGRITY (ART. 32(1)(b) GDPR) 10

4.2.1 Disclosure control .... **Fehler! Textmarke nicht definiert.**
4.2.2 Input control .... **Fehler! Textmarke nicht definiert.**

4.3 AVAILABILITY AND RESILIENCE (ART. 32(1)(B) AND (C) GDPR) 12

4.3.1 Rapid recoverability 13

4.4 PROCEDURES FOR REGULAR REVIEW, ASSESSMENT, AND EVALUATION (ART. 25(1) GDPR; ART. 32(1)(D) GDPR) .... **FEHLER! TEXTMARKE NICHT DEFINIERT.**

4.4.1 Data protection management 14
4.4.2 Incident response management 14
4.4.3 Privacy-friendly default settings (Art. 25(2) GDPR) **Fehler! Textmarke nicht definiert.**
4.4.4 Order control .... **Fehler! Textmarke nicht definiert.**

4.5 PSEUDONYMIZATION AND ENCRYPTION (ART. 32(1)(A) GDPR) 13 A GDPR) .... **FEHLER! TEXTMARKE NICHT DEFINIERT.**

4.5.1 Pseudonymization 15
4.5.2 Encryption at file level: 15
4.5.3 Encryption at hardware level: 15

5 COOPERATION **15**

1 Introduction

The EU General Data Protection Regulation (GDPR) contains guidelines on how personal data should be handled from a technical and organizational perspective. This serves the purpose of data security. Data security is therefore a further and complementary aspect of data protection.

The requirements for data security are regulated by law in Art. 32 (1) GDPR. These provisions require that technical and organizational measures be taken to ensure the protection of personal data.

The law specifies various areas of control, each of which 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 Art. 28 (3) (c) GDPR.

2 Organizational matters

medica Medizintechnik GmbH guarantees written documentation of the current level of data protection as well as written work instructions, guidelines, and information sheets for employees. Employees involved in data processing are bound to data secrecy and confidentiality in accordance with Art. 28 (3) (2) (b), 29, and 32 (4) GDPR.

Some security measures relating to this area in the following checklist are not shown separately, as they fall under the responsibility of any subcontractors or are not published in detail for security reasons.

3 Data protection management

Measures to ensure that personal data and persons working with such data have been informed of or are obliged to comply with organizational requirements for handling such data.

The following measures have been taken within the company:

- • The roles of DSKO and (e)DSB in the area of data protection have been defined and the scope of their respective tasks has been communicated.
- • The expertise of the (e)DSB is ensured.
- • There is an onboarding process for new employees that takes data protection issues into account and regulates the assignment of rights by the IT department.
- • All employees have signed a confidentiality agreement.
- • All new employees receive information on data protection when signing the confidentiality agreement. Furthermore, employees have been bound to data secrecy.
- • Employees are regularly trained in data protection-compliant behavior through data protection training/awareness measures.
- • There is an offboarding process for dealing with departing employees and the withdrawal of rights/operating resources granted.

4 Protective matter

The following points describe the technical and organizational measures implemented by medica Medizintechnik GmbH.

4.1 Confidentiality (Art. 32 (1) (b) GDPR)

4.1.1 Entry control

Access control includes measures designed to prevent unauthorized persons from accessing data processing equipment used to process or use personal data (e.g., automatic access control systems, manual locking systems, video surveillance, security personnel, etc.).

TT Cloud-specific measures by Microsoft Azure:

- Physical security measures in Microsoft Azure data centers, including:
- Strict access controls with biometric identification and multi-factor authentication
- 24/7 monitoring by security personnel
- Video surveillance and alarm management
- Redundant power supply, air conditioning, and fire protection systems
- Certifications in accordance with ISO 27001, SOC 2

Measures taken by our company:

- Selection of Azure regions within the EU to comply with the GDPR
- Use of Azure Security Center to monitor security-related events
- Restriction of administrative access to Azure administrator accounts (zero trust principle)
- Logging of all access processes to the cloud resource
- Regular review of Microsoft's security reports and certifications

medica IT/ development-specific measures

- Type of development:
  - It is a detached building complex, the property is openly accessible.
  - It is a property with factory premises, the property is openly accessible.
  - It is a closed development.
  - There is a building security concept in place.
  - Access to the company premises is freely accessible.
  - There is a visitor management system in place and all visitors to the company must register at the central reception and may only enter non-public areas when accompanied. In addition, visitors are recorded in the visitor log.
- The company uses an automatic access control system; authorized persons use chip cards/tokens for verification.
- The company uses security locks in some areas/exclusively.
- The company has a manual locking system.

- There is a documented key assignment system for keys/tokens/chip cards.
- The company uses a locking system with a code lock.
- The company has a personnel control system that checks all visitors.
- Light barriers/motion detectors connected to the company security center are used to monitor the company premises and building and alert the security center.
- The administration and maintenance of the mechanical access control systems is regulated and documented.
- Personal data is stored in the access control systems so that it is possible to trace who entered and, if applicable, left a specific area at what time (possibly including evaluation in the event of security breaches).
- There are security zones of varying classification and sensitivity.
- The building complex is closed outside business hours and can only be opened manually by authorized persons.
- The company's offices are separately secured by an electronic security lock /
- Entsprechende Regelungen für den Zutritt von externen Personen (Wartungsdienst; Reinigungsdienst; Besucher) sind implementiert. Externe Personen, die Zutritt zum Rechenzentrum benötigen, halten sich ausschließlich in Beisein der IT-Administration im Rechenzentrum auf.
- Server room:
  - The company servers are operated in a locked and access-secured room; only authorized persons have access to this server room.
  - Measures have been taken to monitor the server room/data center (motion detectors).

4.1.2 Access control

Measures that are suitable for preventing data processing systems from being used by unauthorized persons (e.g., authentication measures, VPN connections)

TT- Cloud specific measures:

- Identity and access management (IAM)
  - Use of Microsoft Entra ID (formerly Azure AD) for central management of user rights
  - Role-based access control (RBAC) for assigning minimum rights (least privilege principle)
  - Regular review and adjustment of permissions
- Authentication security
  - Multi-factor authentication (MFA) for all administrative and sensitive access
- Securing the login process
  - Single sign-on (SSO) for secure and centralized authentication
  - Use of Azure Password Protection to enforce secure passwords and prevent weak passwords
  - Logging of login attempts via Microsoft Defender for Cloud

- Network-based access controls
    - Restriction of access to critical services through Azure Virtual Network (VNet) and Network Security Groups (NSG)

medica IT specific masures:

- Access to the IT systems is only possible with individual user names and passwords.
- Access to the IT systems is only possible for employees of the company who have been granted access authorization.
- An allocation process for access rights has been defined with the management, and approval is granted in accordance with this defined process.
- User logins and the respective time of login are logged.
- There is a formal user registration and deregistration process for all information systems and services for the assignment and revocation of access authorizations.
- It is ensured that only authorized persons have logical access to the network components.
- Sufficient measures are in place for the identification and authentication of external maintenance personnel (e.g., secure password protection, separate user account).
- Initial passwords are used and a change is enforced by the system during the first login. In addition, employees are regularly asked to change their passwords. Incorrect password entries are logged.
- Any (remote) maintenance operations are monitored and logged. The user has the option to terminate the connection at any time.
- Access to the company network from outside is via encrypted connections (e.g., VPN) and separate authentication.
- Biometric methods are used for authentication.
- User profiles are assigned to the respective IT systems within the company.
- Anti-virus solutions are used on all IT systems within the company.
- The company shuts down unnecessary services.
- The company protects its IT infrastructure with software and hardware firewalls.
- •Authentication is performed using a user name and password.
- The number of persons with access authorization is kept to a minimum.
- There is a functional restriction on the use of client systems and computer workstations (restrictive assignment of rights).
- The IT department uses network monitoring with alerts.
- A separate guest Wi-Fi network is used so that access to the company network is not possible via this network.

4.1.3 Control access

Measures that ensure that persons authorized to use a data processing system can only access data for which they have access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, and after storage (e.g., automatic verification of *access authorization by means of a password, differentiated access authorizations for application programs).*

TT-Cloud specific measures:

Authorization concept & role management

- Implementation of a role-based access concept (RBAC)
- Least privilege principle and need-to-know principle:
  - Only necessary authorizations for employees and service providers
  - Regular review and adjustment of roles
- Automatic deactivation of inactive user accounts

Data security & access restriction

- Encryption of data during storage and transmission with Azure Storage Encryption (AES-256) and TLS 1.2/1.3

  Access to medical patient data is restricted to authorized user groups only

Logging & monitoring

- Logging and monitoring of all access via Microsoft Defender for Cloud
- Use of Azure Monitor and Log Analytics to detect anomalies and unauthorized access

Session management & access rstriction

- Automatic session timeouts for unused sessions

medica IT/ development specific measures:

- There is a role and authorization concept; authorization checks are performed on the basis of this concept.
- There is a separation of billing and customer master data implemented in the authorization concept.
- Authorization is granted based on the “need-to-know principle.”
- There is an instruction to users on how to handle the IT systems when leaving their workstation (locking).
- Personal data can only be read, copied, modified, or deleted within the scope of the authorization concept.
- The IT department ensures that continuously updated virus protection software is used.
- Incoming email traffic is checked for viruses and spam by a central virus protection and spam filter system.
- There is a password policy that takes into account the current recommendations of the BSI. The minimum criteria are defined by the system.
- A software-based exclusion (authorization concept) is established.
- User access options are restricted to the required scope.
- Restrictive access authorizations/project-related accesses are established.
- There is a coordinated authorization assignment procedure in place.

- The IT department has created IT security guidelines/policies and trained employees in their use.
- Data is encrypted at the file/directory level.
- There are instructions for employees on how to handle data carriers (hard drives, USB sticks, paper forms) that are no longer needed.
- There are instructions on the disposal of devices, including storage media.

4.1.4 Seperation requirement

Measures that ensure that data collected for different purposes can be processed separately (e.g., separation of test and production environments, separation of management network from production network, logical separation, etc.).

Cloud specific measures:

Technical measures for data separation

- Multi-tenant architecture in Microsoft Azure:
  - Use of separate Azure subscriptions and resource groups to separate development, test, and production environments
- Database and storage type separation:
  - Separation of sensitive patient data from general system or log data
  - Use of separate databases and access restrictions for patient data
- Access control at the application level:
  - Implementation of role-based access restrictions (RBAC) to separate user groups (e.g., administrators, therapists, technical staff)

medica IT/ development-specific measures:

- The company uses a testing and approval procedure for software products.
- The company separates the production environment from the testing and development environment.
- The management network is separated from the production network.
- The system landscape is logically separated in accordance with the role and authorization concept.
- The company separates test data from production data.
- The development and production programs are separated from each other.
- There is a change management system with a differentiated approval process.
- A software-based exclusion (client separation) is established.
- Measures for anonymization/pseudonymization are used.

4.2 Integrity (Art.32(1)(b) GDPR)

4.2.1 Control of disclosure

Measures that ensure that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or during transport or storage on data carriers, and that it is possible to check and determine to which locations personal data is to be transmitted by data transmission facilities (e.g., destruction, deletion, and encryption of data carriers, VPN encryption, hardware encryption).

Cloud specific measures

Technical measures to secure data transmission

- End-to-end encryption of all data transfers:
    - TLS 1.2/1.3 for all network connections
    - Azure Storage Encryption for stored data
- Secure API and system communication:
    - REST API with JWT authentication token

Organizational measures to control data transfer

- Strict access controls for data exports:
    - Only authorized users may export or transfer data
    - Approval procedure for external data transfers
    - Logging and tracking of all data transfers
- Contract management and data processing agreements with external recipients:
    - Conclusion of data protection agreements with all external service providers
    - Regular data protection audits of external recipients

medica IT/ development specific measures:

- When data is transferred, only approved encryption solutions/VPN tunnels are used for transmission.
- There is a company-wide classification concept for data with regard to confidentiality levels.
- Access to data and files via the web is via an SSL-encrypted connection.
- Regulation of system communication traffic (central firewall, exclusive WAN (Wide Area Network) connections with access controls), logging (user authentication, time stamp).
- The transport connection is only established between defined systems secured by certificates.
- Employees can only access the company network from their mobile workstations/home workstations via VPN access.
- Employees can only use services that have been approved by IT.
- Data carriers and paper documents are destroyed in a controlled manner in accordance with DIN 66399.

4.2.2 Input control

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, modified, or deleted in data processing systems (e.g., user profiles, logging of entered data (processing log), failed login attempts, administrative activities via a ticket system).

TT-cloud specific measures

- *User identification & authentication:*
  - *Individual user accounts for all entries (no anonymous or shared accounts)*
- *Field-based validation & verification mechanisms:*
  - *Secure entries through mandatory fields, plausibility checks, and value ranges*
  - *Automatic warning messages for incorrect entries*
  - *Spring JPA repositories and JDBC with exclusively named or indexed/positional parameters. (The parameters are not built directly into the SQL string, but are processed securely as variables, thereby ruling out SQL injections.)*

Organizational measures for input control

- Clear distribution of roles and authorization concepts for data changes
- Training of employees in secure and correct data entry
- Regular data protection and security checks of input procedures

medica IT/ development specific measures:

- System-based plausibility checks are implemented in the company.
- A role and authorization concept is in place.
- All employees have user profiles that are adapted to their scope of authorization.
- The company logs the data entered (processing log).
- Access logging takes place for (remote) maintenance activities.
- User identifications are established in the IT systems.
- Firewall logging (TCP/IP) is carried out.
- The systems are configured in such a way that failed login attempts are logged.
- User logging is activated in Active Directory.

4.3 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 restored in the event of a physical or technical incident (e.g., UPS and emergency power generator, alarm system, redundant data storage (RAID hard disk systems), firewalls, virus protection programs, multiple incremental database and system backups, data backup concepts).

TT-cloud specific measures:

Technical measures to ensure viability
High availability & redundancy

- Use of Azure Availability Zones & Region Replication to ensure operation even in the event of disruptions

Backup & Disaster Recovery

- Automated, encrypted backups with Azure Backup & Site Recovery
    - Daily backups with defined retention policies
    - Storage in Azure Blob Storage solutions
- Disaster recovery strategies:
    - Regular testing of emergency plans (disaster recovery tests)
    - Establishment of a business continuity plan (BCP) for rapid recovery after failures
    - Emergency manual for system recovery

DDoS and attack protection

- DDoS Protection Standard to defend against overload attacks
- Firewall & Web Application Firewall (WAF) to ensure the availability of cloud services

Organizatipnal measures to ensure availability

- Defined emergency processes and escalation levels in the event of system failures
- Regular training for administrators and IT staff on disaster recovery
- Regular review of system load and capacity planning

medica IT/ development specific measures:

- Personal data is always available and protected against accidental destruction or loss by regular data backups.
- A data backup concept with regular backups has been established. The backups are stored in separate areas and in encrypted form.
- A backup/recovery concept has been developed and established.
- An emergency manual has been implemented and is updated regularly.
- The server rooms/data centers are specially protected by a separate access control system.
- The company uses fire protection devices in the building to secure the IT systems.
- The server rooms/data centers have redundant power supplies, both geo-redundant and dual power supplies.
- The server rooms/data centers have their own monitoring systems, which are connected directly to the IT department.

- Uninterruptible power supplies, including surge protection and emergency power generators, are used.
- A suitable extinguishing system (gas extinguishing system) is available in the server room/data center. There is also a fire/smoke alarm system.
- The building and the server room/data center have lightning protection systems.
- Air conditioning is used in the server room/data center. The air conditioning technology is documented by the company.
- The network components are distributed across several protected areas for the purpose of minimizing risk/downtime.
- Surge protection is integrated.
- The alarm system used is directly connected to the control center, plant security, fire department, security service, etc.
- No flammable materials/objects are stored in the server room/data center.
- The server rooms/data center are designed and planned in such a way that there are no water pipes.
- The server systems use RAID hard disk systems to ensure reliability.

4.3.1 Rapid recoverability

Requirement: Measures to ensure that personal data is protected against accidental destruction or loss and can be quickly restored in the event of a physical or technical incident. (Art. 32 (1) (c) GDPR)

TT-cloud specific measures:

Backup- and recovery strategy

- Automated data backup with Azure Backup & Site Recovery
  - Daily automated backups with versioning
  - Encrypted backups with AES-256 and key management via Azure Key Vault
- Recovery within defined RTO and RPO times
  - Recovery Time Objective (RTO): Maximum recovery time of 24 hours
  - Recovery Point Objective (RPO): Maximum data loss of 24 hours

Disaster recovery & emergency management

- Azure Site Recovery for automated failover scenarios
  - Emergency recovery plans for critical systems
  - Failover to an alternative region in the event of critical failures
- Regular recovery tests
- Real-time monitoring with Azure Monitor
  - Automatic detection of system failures and threats
  - Notification of administrators & escalation processes

Organizational measures for rapid recovery

- Contingency plan & escalation guidelines for IT failures
  - oDefined responsibilities & contact chains in case of emergency
  - Training of employees in dealing with system failures
  - Regular audits & reviews of recovery processes

medica IT/ development specific measures:

- A backup is available
- A backup/recovery concept has been developed and established.

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

4.4.1 Data protection management

medica Medizintechnik GmbH operates a data protection management system (DPMS) in accordance with the requirements of Art. 5 (2) GDPR. It is based on the PDCA cycle and is therefore subject to ongoing effectiveness monitoring.

4.4.2 Incident-response-management

A procedural approach to security incidents has been implemented. In the event of an incident, employees immediately inform IT or their supervisor. This is followed by consultation with the data protection officer. The processing of incidents is ensured by appropriate substitution arrangements.

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

As a matter of principle, only data that is appropriate and necessary for business activities is collected and processed. Automated data collection and processing procedures are designed in such a way that only the necessary data can be collected.

4.4.4 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 (e.g., confidentiality or data secrecy obligations, especially for IT administrators, contract for order processing in accordance with Art. 28 GDPR, blocking external access, e.g., for remote maintenance by external parties, granting of restrictive access authorizations, involvement of the data protection officer/information security officer, etc.).

Requirements for entering into a subcontracting relationship:

- Contract for commissioned data processing in accordance with Art. 28 (3) GDPR.
- German service providers have appointed a company data protection officer and ensure that they are appropriately and effectively integrated into the relevant operational processes through the data protection organization.
- Description of checks and audits.
- Assignment of individual orders. Confirmation of verbal orders.
- Only restrictive access authorizations are granted to the relevant technical environments. In the case of external access to the system, access is deactivated or blocked after the end of the cooperation.

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

4.5 Pseudonymization and encryption (Art. 32 (1) (a) GDPR)

4.5.1 Pseudonymization

If direct personal reference is not necessary, pseudonymization is used where possible and where the effort involved is proportionate to the intended purpose of protection (data minimization).
In addition, measures for privacy by design and privacy by default, including appropriate training measures in the product area, are implemented in accordance with the principles of data avoidance and data minimization.

4.5.2 Encryption at file level:

(e.g., encryption of confidential documents, encrypted transmission channels via VPA, establishment of transport connections only between defined and certificate-secured systems, data transmission from the website via SSL encryption).

- State-of-the-art encryption technologies are used. This means that TLS (SSL) encryption, hash encryption, etc. are used.

4.5.3 Encryption at hardware level:

(*e.g., encryption of hard drives in notebooks, password-protected hardware, etc.)*

State-of-the-art encryption technologies are used for the hardware level (e.g., Bitlocker).

5 Cooperation

In order to comply with the data protection requirements of the GDPR, medica Medizintechnik GmbH works together with DDSK GmbH. In addition to drawing up guidelines and practical aids, DDSK GmbH advises medica Medizintechnik GmbH on all matters relating to data protection and, in the person of Mr. Stefan Fischerkeller, provides the company with an external data protection officer in accordance with Art. 37 GDPR.

DDSK GmbH
Stefan Fischerkeller
Dr. Klein-Straße 29, 88069 Tettnang
Tel. 07542 / 949 21 00
E-Mail: datenschutz@thera-trainer.com
Web: www.ddsk.de

DDSK
DEUTSCHE
DATENSCHUTZKANZLEI

Maximilian Musch
Master of Arts, certified expert data protection officer (udis)
German Data Protection Law Firm – Maximilian Musch
Richard-Wagner-Straße 2, 88094 Oberteuringen
Tel.: 07542 / 949 21 02
E-Mail: musch@ddsk.de
Web: www.ddsk.de