

# Agreement on the processing of personal data

between	and
OPED GmbH	the company responsible for the use of the software
Medizinpark 1	(responsible party)
83626 Valley/Oberlindern	

hereinafter referred to as **the Contractor**                      hereinafter referred to as **the Client**

## Table of Contents

1	Introduction, scope, definitions .....	3
2	Subject matter and duration of processing.....	3
2.1	Subject.....	3
2.2	Duration .....	3
2.3	Type and purpose of processing.....	3
2.4	Categories of data subjects and type of data.....	3
3	Obligations of the contractor .....	3
4	Technical and organizational measures.....	4
5	Regulations on the correction, deletion, and blocking of data .....	5
6	Subcontracting .....	5
7	Rights and obligations of the client.....	6
8	Notification obligations .....	6
9	Instructions .....	6
10	Termination of the contract .....	7
11	Remuneration .....	7
12	Special right of termination.....	7
13	Liability.....	7
14	Miscellaneous.....	7
	Appendix 1 – Technical and organizational measures.....	9
1	TECHNICAL AND ORGANIZATIONAL MEASURES .....	9
1.1	Guideline.....	9
1.2	Organization of information security.....	9
1.3	Personnel security .....	10
1.4	Management of values .....	10
1.5	Access control .....	10
1.6	Cryptography .....	11
1.7	Physical and environmental security.....	11
1.8	Operational security.....	11
1.9	Communication security .....	12

1.10	Procurement, development, and maintenance of systems.....	12
1.11	Supplier relationships .....	13
1.12	Handling of information security and data protection incidents .....	13
1.13	Information security aspects of business continuity management .....	13
1.14	Compliance .....	13
2	FURTHER MEASURES.....	14
2.1	Procedure directories .....	14
2.2	Legal impact assessments .....	14
2.3	Employee training and awareness .....	14
3	Company regulations .....	14
	Appendix 2 – Approved subcontractors.....	15
	Appendix 3 – Authorized representative.....	16
	Appendix 4 – Data protection officer.....	17
	Appendix 5 – Certifications .....	18

## 1 Introduction, scope, definitions

- (1) This contract governs the rights and obligations of the client and the contractor (hereinafter referred to as "the parties") in connection with the processing of personal data on behalf of the client.
- (2) This contract applies to all activities in which employees of the contractor or subcontractors commissioned by the contractor process personal data of the client.
- (3) Terms used in this contract shall be understood in accordance with their definitions in the EU General Data Protection Regulation. Insofar as declarations in the following must be made "in writing," this refers to the written form as defined in Section 126 of the German Civil Code (BGB). Otherwise, declarations may also be made in other forms, provided that adequate verifiability is ensured.

## 2 Subject matter and duration of processing

### 2.1 Subject matter

Provision of image recognition software for documentation and post-processing.

### 2.2 Duration

The order is issued for an indefinite period and can be terminated by either party with 30 days' notice to the end of the month. The right to terminate the contract without notice remains unaffected.

### 2.3 Type and purpose of processing

The processing is of the following nature:

Collection, organization, structuring, storage (e.g., reorganization in memory), retrieval, consultation, use, alignment or combination, restriction, erasure, or destruction of data (e.g., duplicates).

Purpose of processing:

- Provision, operation, hosting, maintenance, and support of the software.

### 2.4 Categories of data subjects and type of data

#### Data subjects

The client's patients  
Users

#### Types of data

Patient number, date of birth, height.  
Information on user and device identification

## 3 Obligations of the contractor

- (1) The contractor shall process personal data exclusively as contractually agreed or as instructed by the client, unless the contractor is legally obliged to process the data in a specific manner. If such obligations exist, the contractor shall inform the client of this prior to processing, unless such notification is prohibited by law. Furthermore, the contractor shall not use the data provided for processing for any other purposes, in particular not for its own purposes.
- (2) The contractor confirms that it is aware of the relevant general data protection regulations. It shall observe the principles of proper data processing.
- (3) The contractor undertakes to maintain strict confidentiality during processing.
- (4) Persons who may gain knowledge of the data processed on behalf of the client shall be required to sign a written confidentiality agreement, unless they are already subject to a relevant confidentiality obligation by law.

- (5) Confidentiality obligation, reference to Section 203 of the German Criminal Code (StGB): The contractor is obliged to maintain confidentiality, even after completion of the order. This obligation applies to everything that becomes known to the contractor in the course of its activities for the client. This does not apply to facts that are obvious or do not require confidentiality due to their significance.
- (6) The contractor guarantees that the persons employed by it for processing have been made familiar with the relevant provisions of data protection and this contract before the start of processing. Appropriate training and awareness-raising measures shall be repeated at regular intervals. The contractor shall ensure that persons employed for order processing are continuously instructed and monitored in an appropriate manner with regard to the fulfillment of data protection requirements.
- (7) In connection with the commissioned processing, the contractor shall support the client in creating and updating the record of processing activities and in carrying out the data protection impact assessment. All necessary information and documentation shall be kept available and forwarded to the client immediately upon request.
- (8) If the client is subject to an inspection by supervisory authorities or other bodies, or if data subjects assert their rights against the client, the contractor undertakes to support the client to the extent necessary, insofar as the processing on behalf of the client is affected.
- (9) The contractor may only provide information to third parties or the data subject with the prior consent of the client. It shall forward any inquiries addressed directly to it to the client without delay.
- (10) Where required by law, the contractor shall appoint a competent and reliable person as data protection officer. It must be ensured that the data protection officer has no conflicts of interest. In cases of doubt, the client may contact the data protection officer directly. The contractor shall immediately provide the client with the contact details of the data protection officer or explain why no officer has been appointed. The contractor shall immediately inform the client of any changes in the person or internal tasks of the officer.
- (11) Order processing shall always take place within the EU or the EEA. Any transfer to a third country may only take place with the express consent of the client and under the conditions set out in Chapter V of the General Data Protection Regulation and in compliance with the provisions of this contract.

## 4 Technical and organizational measures

- (1) The data security measures described in Appendix 1 are binding. They define the minimum required by the contractor.
- (2) The data security measures may be adapted in line with technical and organizational developments, provided that the level agreed here is not reduced. The contractor shall implement any changes necessary to maintain information security without delay. The client shall be notified of any changes without delay. Significant changes shall be agreed between the parties.
- (3) If the security measures taken do not or no longer meet the client's requirements, the contractor shall notify the client immediately.
- (4) The contractor guarantees that the data processed in the order will be strictly separated from other data stocks.
- (5) Copies or duplicates shall not be made without the knowledge of the client. This does not apply to technically necessary temporary reproductions, provided that this does not impair the level of data protection agreed here.
- (6) When processing data in private homes, the contractor shall ensure that a level of data protection and data security in accordance with this contract is maintained and that the client's control rights specified in this contract can also be exercised without restriction in the private homes concerned. The processing of data on behalf of the client using private devices is not permitted under any circumstances.

- (7) Dedicated data carriers originating from the client or used for the client shall be specially marked and subject to ongoing management. They shall be stored appropriately at all times and shall not be accessible to unauthorized persons. Entries and exits shall be documented.
- (8) The contractor shall ensure a procedure for regularly reviewing, assessing, and evaluating the effectiveness of the technical and organizational measures to ensure the security of processing in accordance with Art. 32 (1) lit. d GDPR.

## **5 Regulations on the correction, deletion, and blocking of data**

- (1) Data processed within the scope of the contract shall only be corrected, deleted, or blocked by the contractor in accordance with the agreement made or on the instructions of the client.
- (2) The contractor shall comply with the client's instructions at all times and even after the termination of this contract.

## **6 Subcontracting**

- (1) Currently, the subcontractors named in Appendix 2, with their names, addresses, and the content of their contracts, are engaged in the processing of personal data to the extent specified therein and have been approved by the client. The other obligations of the contractor toward subcontractors set forth herein remain unaffected.
- (2) The client agrees that the contractor may engage subcontractors. The contractor shall inform the client before engaging or replacing a subcontractor.  
The client has the right to object in writing to the use of the subcontractor within two weeks of receiving information about the subcontractor for good cause. If no objection is made within the specified period, this shall be deemed to constitute the client's consent to the use of this subcontractor.
- (3) Subcontractors shall be contractually bound to at least the same data protection obligations as those agreed in this contract. Upon request, the client shall be granted access to the relevant contracts between the contractor and subcontractors.
- (4) The rights of the client must also be effectively enforceable against the subcontractor. In particular, the client must be entitled to carry out checks at any time to the extent specified herein, including checks on subcontractors, or to have such checks carried out by third parties.
- (5) The responsibilities of the contractor and the subcontractor must be clearly distinguished from one another.
- (6) Further subcontracting by the subcontractor is not permitted.
- (7) The contractor shall select the subcontractor with particular regard to the suitability of the technical and organizational measures taken by the subcontractor.
- (8) The forwarding of data processed on behalf of the client to the subcontractor is only permitted if the contractor has documented that the subcontractor has fulfilled its obligations in full. The contractor shall submit the documentation to the client without being asked to do so.
- (9) The commissioning of subcontractors who do not perform processing on behalf of the client exclusively from within the EU or the EEA is only possible if the conditions set out in Chapter 3 (11) and (12) of this contract are met. In particular, it is only permissible if and for as long as the subcontractor offers adequate data protection guarantees.
- (10) Subcontracting relationships within the meaning of this contract are only those services that are directly related to the provision of the main service. Ancillary services, such as transport, maintenance, and cleaning, as well as the use of telecommunications services or user services, are not covered. The contractor's obligation to ensure compliance with data protection and data security in these cases remains unaffected.
- (11) If the subcontractor fails to comply with its data protection obligations, the contractor shall be liable to the client.

## 7 Rights and obligations of the client

- (1) The client is solely responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.
- (2) The client shall issue all orders, partial orders, or instructions in writing. In urgent cases, instructions may be given verbally. The client shall confirm such instructions in writing without delay.
- (3) The client shall inform the contractor immediately if it discovers any errors or irregularities when checking the results of the order.
- (4) The client is entitled to monitor compliance with the data protection regulations and the contractual agreements at the contractor's premises to a reasonable extent, either itself or through third parties, in particular by obtaining information and inspecting the stored data and data processing programs, as well as by carrying out other on-site checks. The contractor shall grant the persons entrusted with the inspection access and inspection rights to the extent necessary. The contractor is obliged to provide the necessary information, demonstrate processes, and provide evidence required for the inspection.
- (5) Controls at the contractor's premises must be carried out without avoidable disruption to its business operations. Unless otherwise indicated for urgent reasons to be documented by the client, checks shall take place after reasonable notice and during the contractor's business hours, and no more frequently than once every 12 months. If the contractor provides evidence of the correct implementation of the agreed data protection obligations as provided for in Section 4 (8) of this contract, checks shall be limited to random samples.

## 8 Notification obligations

- (1) The contractor shall notify the client immediately of any breaches of personal data protection. Justified cases of suspicion must also be reported. The notification must contain at least the information specified in Art. 33 (3) of the General Data Protection Regulation.
- (2) Significant disruptions in the execution of the order and violations of data protection provisions or the provisions of this contract by the contractor or persons employed by the contractor shall also be reported immediately.
- (3) The contractor shall immediately inform the client of any inspections or measures taken by supervisory authorities or other third parties insofar as these relate to order processing.
- (4) The contractor undertakes to support the client to the extent necessary in fulfilling its obligations under Articles 33 and 34 of the General Data Protection Regulation.

## 9 Instructions

- (1) The client reserves the right to issue comprehensive instructions with regard to the processing on its behalf.
- (2) The client and contractor shall name the persons exclusively authorized to issue and accept instructions in Appendix 3.
- (3) In the event of a change or long-term unavailability of the designated persons, the other party shall be notified immediately of their successors or representatives.
- (4) The contractor shall immediately notify the client if, in its opinion, an instruction issued by the client violates legal regulations. The contractor is entitled to suspend the execution of the relevant instruction until it has been confirmed or amended by the responsible person at the client.
- (5) The contractor shall document any instructions given to it and their implementation.

## 10 Termination of the contract

- (1) Upon termination of the contractual relationship or at any time at the request of the client, the contractor shall, at the client's discretion, either destroy the data processed in the order or hand it over to the client and then destroy it. All existing copies of the data must also be destroyed. The destruction must be carried out in such a way that even residual information cannot be restored with reasonable effort.
- (2) The contractor is obliged to ensure that subcontractors also return or delete the data without delay.
- (3) The contractor must provide proof of proper destruction and submit it to the client immediately.
- (4) Documentation serving as proof of proper data processing shall be retained by the contractor in accordance with the respective retention periods, even beyond the end of the contract. The contractor may hand it over to the client at the end of the contract to relieve itself of its obligation.

## 11 Remuneration

The remuneration of the contractor is conclusively regulated in the main contract. No separate remuneration or reimbursement of costs shall be made under this contract.

## 12 Special right of termination

- (1) The client may terminate the main contract and this agreement at any time without notice ("extraordinary termination") if the contractor seriously violates data protection regulations or the provisions of this agreement, if the contractor is unable or unwilling to carry out a lawful instruction of the client, or if the contractor refuses to allow the client to exercise its rights of inspection in breach of the contract.
- (2) A serious breach shall be deemed to have occurred in particular if the contractor fails to fulfill or has failed to fulfill the obligations specified in this agreement, in particular the agreed technical and organizational measures, to a significant extent.
- (3) In the event of minor breaches, the client shall set the contractor a reasonable deadline for remedial action. If the remedial action is not taken in good time, the client shall be entitled to extraordinary termination as described in this section.
- (4) The contractor shall be entitled to extraordinary termination if the client objects to the commissioning of a subcontractor in accordance with Section 6 (1) of this contract and no agreement can be reached.

## 13 Liability

- (1) The client and contractor shall be jointly and severally liable for compensation for damages suffered by a person as a result of improper or incorrect data processing within the scope of the contractual relationship.
- (2) Insofar as the damage was caused by the correct implementation of the commissioned service or an instruction given by the client, the client shall indemnify the contractor upon first request against all claims of third parties asserted against the contractor in connection with the order processing.
- (3) The contractor shall only be liable to the client in cases of gross negligence or intent.

## 14 Miscellaneous

- (1) Both parties are obliged to treat all knowledge of business secrets and data security measures of the other party obtained within the scope of the contractual relationship as confidential, even after

the termination of the contract. If there is any doubt as to whether information is subject to confidentiality, it shall be treated as confidential until written approval is given by the other party.

- (2) If the client's property is endangered by measures taken by third parties (e.g., through seizure or confiscation), by insolvency or composition proceedings, or by other events, the contractor shall notify the client immediately.
- (3) Any ancillary agreements must be made in writing.
- (4) The right of retention within the meaning of Section 273 of the German Civil Code (BGB) is excluded with regard to the data processed in the order and the associated data carriers.
- (5) Should individual parts of this agreement be invalid, this shall not affect the validity of the agreement as a whole.

## Appendix 1 – Technical and organizational measures

The following section sets out the technical and organizational measures to ensure data protection and data security that the contractor must implement as a minimum and maintain on an ongoing basis. The aim is to ensure, in particular, the confidentiality, integrity, and availability of the information processed on behalf of the client.

Protection class 2 applies to destruction in accordance with DIN 66399.

1. Organization of information security
2. Personnel security
3. Management of assets
4. Access control
5. Cryptography
6. Physical and environmental security
7. Operational security
8. Communication security
9. Procurement, development, and maintenance of systems
10. Supplier relationships
11. Handling of information security incidents
12. Information security aspects of business continuity management
13. Compliance

### 1 TECHNICAL AND ORGANIZATIONAL MEASURES

The technical and organizational measures established to ensure data protection and data security are described below. The aim is to ensure, in particular, the confidentiality, integrity, and availability of the information processed within the company. The structure is based on the internationally recognized DIN ISO/IEC 27002 standard.

#### 1.1 Guideline

The data protection guideline of OPED GmbH contains the guiding principles of the management regarding the handling of personal data within the company. All employees, freelancers, and supporting companies are obliged to observe these central regulations.

The IT security level achieved by the organizational units, processes, and systems is monitored through a combination of periodic audits and continuous controls.

The monitoring of ongoing operations is carried out in coordination with the security officer.

The security policy is reviewed at least once a year, unless an essential change requires earlier review. This ensures the ongoing adequacy, suitability, and effectiveness of the policy.

The security officer is responsible for the security policy and is responsible for developing, revising, and reviewing it.

#### 1.2 Organization of information security

The managers of OPED GmbH are responsible within their organizational unit for the complete implementation of the IT security principles and for fulfilling the IT security tasks assigned to them.

Information security roles and responsibilities are defined in the IT security organization. Conflicting tasks and areas of responsibility are separated to reduce the possibility of unauthorized or unintentional changes or misuse of our company's assets.

We have a procedure in place that specifies when and by whom relevant authorities are to be notified and when detected data protection and information security incidents are to be reported in a timely manner.

We also maintain ongoing contact with special interest groups to stay informed about changes and improvements in the area of data protection and information security.

In our projects, data protection and data security are an integral part of all phases of our project methodology.

Through our respective guidelines and processes for teleworking and the use of mobile devices, we also ensure data protection and data security in these areas.

### **1.3 Personnel security**

We have carefully selected our employees and checked their suitability for their role in the company. We have defined their responsibilities in job descriptions and regularly check whether employees are fulfilling them. Before starting their employment, all employees sign a confidentiality and data protection agreement that remains in force beyond the end of their employment. Employees receive training in data protection and data security, with refresher courses provided when they change roles. They are therefore aware of their responsibilities in this regard.

In a documented process for the period before, during, and after the termination of employment, we ensure that personal data is protected and data security is guaranteed. This also includes disciplinary measures in the event of a data protection breach.

### **1.4 Management of assets**

All assets (such as operating resources, removable data carriers, notebooks) and information related to personal data are inventoried and maintained by us.

We have appointed persons responsible for protecting these assets, who are responsible for the life cycle of an asset.

Documented rules have been established for the permissible use of our assets. Their return is documented.

Our information and data are classified and labeled based on legal requirements, their value, their criticality, and their sensitivity to unauthorized disclosure or modification.

In accordance with this classification scheme, we have developed and implemented documented procedures for handling our assets, in particular our removable data carriers. We have a documented and regulated process for transporting data carriers to protect them from unauthorized access, misuse, or falsification.

We dispose of data carriers that are no longer required securely, using a documented procedure and certified service providers.

### **1.5 Access control**

We have regulated and documented measures in place to ensure that authorized persons only have access to personal data for which they have the authority to view and process.

Authorizations for access to IT systems are granted through a regulated procedure based on a documented and restrictive authorization concept. We have regulated and implemented access to networks and network services.

We ensure that only authorized users have access to systems and services and that unauthorized access is prevented. In particular, there is a formal process for registering and deregistering users, which enables access rights to be assigned.

We grant administrative rights in a restricted and controlled manner.

We have a documented and regulated process for handling passwords.

The actual and target status of user access rights are regularly compared. If necessary, these are revoked or adjusted.

We restrict access to our data as required and control access to our systems and applications through a secure login procedure. We use a system for the use of secure and strong passwords.

The use of utility programs that could be capable of circumventing system and application protection measures is restricted and strictly monitored.

## **1.6 Cryptography**

The appropriate and effective use of cryptography to protect the confidentiality, authenticity, or integrity of information is ensured. To this end, we have implemented regulations on the use of cryptographic measures within the company, which also include the management of cryptographic keys and are appropriate to the protection requirements.

## **1.7 Physical and environmental security**

We have taken documented and regulated measures to prevent unauthorized persons from gaining access to data processing equipment used to process or use personal data. These include, among other things:

- The business premises are located on the first floor of an office building and are used exclusively.
- Doors to security areas are always closed. Protection is provided by a token-based system.
- Visitors or external service providers are admitted individually.
- Fire safety regulations are observed.
- There are security areas to which only authorized persons have access.
- IT rooms are locked separately and can only be opened by authorized persons.
- Supply facilities are protected against power failures and malfunctions
- The safety of the cabling is observed
- System maintenance is planned or implemented
- The removal and modification of systems and information is regulated.
- The security of systems outside the premises is taken into account.
- The disposal or reuse of operating resources is regulated
- Unattended user devices are protected by encryption
- Clean desk and screen lock policies are implemented.

## **1.8 Operational security**

We have regulated and documented measures in place to ensure the proper and secure operation of information and data processing facilities. These include, among other things, control in the event of changes to information processing facilities, as well as control and regular measurement of our capacities and resources to ensure the availability of the required system performance. For example, the following values are continuously monitored:

- Hard disk status and available memory
- RAID status
- Services and status of all virtual machines
- Failed login attempts
- Storage and main memory usage
- Ethernet utilization in Kbit/s and Mbit/s
- Number of RDP sessions for individual terminal servers
- Firewall throughput and utilization

- Availability of all servers from outside
- Availability and throughput of switches

We have implemented and documented a secure data backup procedure.

Standard maintenance windows are defined. Any additional windows required will be announced at least 10 days in advance.

It is essential in our company to separate development, test, and operating environments from each other, so we pay particular attention to this.

Measures for detection, prevention, and recovery to protect against malware have been taken and are regularly updated.

We have centrally monitored and protected event logging and have taken measures to protect privacy in the event that sensitive personal data is stored. All logging facilities and log information, including administrator and operator logs, are protected against manipulation and unauthorized access.

Our clocks are synchronized centrally with a single reference time source.

We have a centralised procedure for the controlled installation of software on systems within our company.

We have a list of our technical assets and a regulated, documented procedure for dealing with technical vulnerabilities, which includes our patch management with defined responsibilities.

Regulations for restricting software installations are implemented centrally by us.

In the event of an audit of our information systems, we have defined measures to minimize disruptions to business processes as far as possible.

## **1.9 Communication security**

The security of personal data and information stored in our networks and network services is essential. We have therefore implemented documented measures to manage, control, and secure our networks.

Information services, users, and information systems are kept separate from each other as required.

We have guidelines and procedures for information and data transmission, as well as agreements for the transmission of information to external parties.

Our electronic data transmission is adequately protected. Among other things, we have taken measures to protect data from unauthorized access, modification, or denial of service in accordance with the classification scheme adopted by the organization.

To protect our data, we enter into confidentiality or non-disclosure agreements as required, which we review regularly.

## **1.10 Procurement, development, and maintenance of systems**

We ensure that data and information security is an integral part of the entire life cycle of our systems. This also includes the requirements for and security of information systems that provide services via public networks. Transactions in application services are protected as required. In addition, we have established a procedure for managing system changes to ensure the integrity of the system, applications, and products from the early design stages through to all subsequent maintenance work. When changes are made to operating platforms, business-critical applications are reviewed and tested to ensure that there is no negative impact on organizational security, including that of customer applications. We have a controlled process for analyzing, developing, and maintaining secure IT systems.

Acceptance test programs and associated criteria are defined for new information systems, updates, and new versions. Our test data is carefully selected, protected, and controlled.

### **1.11 Supplier relationships**

We carefully select our suppliers in advance and check their suitability with regard to data and information security.

Documented agreements ensure the protection and confidentiality of our assets and data. Suppliers are obliged to take technical and organizational measures to guarantee this.

There is regulated and user-defined access authorization to the values and data that are absolutely necessary for the respective supplier.

Suppliers may only commission other suppliers with our consent in order to ensure a secure supply chain.

We regularly review our suppliers' data protection and data security measures to maintain the agreed level. The assigned authorizations are also subject to constant documented control.

Upon termination of the supplier relationship, suppliers are obliged to destroy the data and values received from us. In addition, the obligation to maintain confidentiality applies indefinitely.

### **1.12 Handling of information security and data protection incidents**

Our company has a regulated, documented process for handling information security and data protection incidents to ensure a consistent and effective approach in this regard. Employees are required to report all data protection and security incidents immediately and receive regular training in this regard. We have installed a reporting system that forwards incidents to an incident response team ( ) to ensure a rapid response. All incidents are documented, classified, and evaluated. The incident response team has precise guidelines on how to respond to an incident.

Together with management, improvement measures are regularly discussed and implemented based on the findings and evidence gathered from an incident.

### **1.13 Information security aspects of business continuity management**

As part of information security, the availability of systems is specifically assessed and documented. We derive technical and organizational requirements, such as redundant systems/connections or appropriate planning, from the requirements and implement them consistently and in a controlled manner. A comprehensive emergency plan provides the framework for the appropriate instructions for selected documented emergency scenarios. Ongoing, updated exercise plans for testing the measures in place and documenting the implementation of appropriate tests round out our emergency management system. All servers and storage systems come with a minimum 36-month manufacturer's warranty.

### **1.14 Compliance**

We have determined, documented, and kept up to date all relevant legal, regulatory, self-imposed, or contractual requirements, as well as our company's procedures for complying with these requirements.

Appropriate procedures have also been implemented to ensure compliance with legal, regulatory, and contractual requirements relating to intellectual property rights and the use of copyright-protected software products.

In accordance with legal, regulatory, contractual, and business requirements, we protect records and personal data as necessary. Annual activity reports from the data protection officer document the measures taken.

We observe the regulations on cryptographic measures for this purpose.

To ensure the protection of our information and data, we regularly conduct independent reviews of our information security and data protection levels, our security and data protection guidelines, and our compliance with technical requirements.

## **2 FURTHER MEASURES**

### **2.1 Procedure directories**

An up-to-date processing overview and procedure directories are available.

### **2.2 Legal impact assessments**

Where required by law, procedures are identified on the basis of predefined risk criteria and levels before they are put into operation and compared with the protective measures. The data protection assessments made in this way are incorporated into the implementation of the measures and documented.

### **2.3 Training and awareness-raising for employees**

Employees receive regular documented training and awareness-raising on data protection and data security issues.

## **3 Company regulations**

The following information security and data protection regulations, among others, are in place within the company:

- Guideline on data subject rights
- Data protection management system manual
- Risk analysis and treatment policy
- Employee onboarding
- Employee offboarding
- Order Processing Policy
- Authorization Policy
- Data protection emergency policy
- Contact persons in the event of a data protection emergency
- Data archiving and deletion policy
- IT usage policy
- Overview of data classification and processing

## Appendix 2 – Approved Subcontractors

- Microsoft Azure (data center provision)
  - Microsoft Deutschland GmbH  
Walter-Gropius-Strasse 5  
80807 Munich
  -
- Lynx SFT, s.r.o (in-app protection)
  - CERIT Science Park  
Botanická 68a  
602 00 Brno, Czech Republic

## **Appendix 3 – Authorized representative**

Andreas Engl – Head of Digital Health Solutions

Email: [a.engl@oped.de](mailto:a.engl@oped.de)

Phone:

## **Appendix 4 – Data Protection Officer**

Email: [datenschutz@oped.de](mailto:datenschutz@oped.de)

## Appendix 5 – Certifications

ISO 27001 certificate from OPED GmbH




**CERTIFICATE**

for a management system as per 

### DIN EN ISO/IEC 27001:2024

Evidence of conformity has been furnished.



**OPED GmbH**  
Medizinpark 1  
83626 Valley/Oberlaindern | Germany

**Scope:**  
Digital Health Solution - Development, production, distribution and service of digital preventive and aftercare concepts based on sensor units, mobile devices and central data storage.

Statement of Applicability (SoA): from 02.12.2025

**Certificate registration No.:**  
73 121 8001

**Certificate valid from:**  
2026-03-02 **to:** 2029-02-27

**previous certificate was valid until:**  
2026-02-27






*Dr. Ponick*

Dr. M. Ponick  
Head of Certification body  
Release, Darmstadt      2026-03-02  
Certification Body of TÜV Hessen



Page 1 of 1  
This certification confirms the introduction and maintenance of the Management system specified above and is monitored regularly. The current validity is verifiable at [www.proficert.de](http://www.proficert.de). Original certificates contain a glued hologram.  
TUV Technische Überwachungs-Hessen GmbH, Robert-Bosch-Strasse 18, 64293 Darmstadt, Germany Phone +49 6151 800331 Rev-GB-2508 Translation of German original