Order Data Processing Agreement

Seca remote support for seca connect 103

Preliminary remarks

With the seca software (hereinafter called "**seca software**"), seca offers the Client a solution with which the measured values of seca devices can be processed on the PC, significantly increasing the quality of a medical examination. For the use of seca Software, seca offers its Clients support in the form of remote access via the Internet. The parties agree that privacy and confidentiality are indispensable for this remote access.

Having said that, the parties have agreed as follows:

1. Definitions

"Personal data" are particulars on personal or material circumstances of a particular or identifiable person. "Data processing on behalf" is the storage, modification, transmission, blocking or deletion of personal data by seca on behalf of the client.

"Instruction" Instruction is the written order from the client directed at certain data protection-related handling of personal data (for example anonymization, blocking, deletion, publication) by seca. The instructions are initially determined by the purchase contract and can then be amended, supplemented or replaced by the client through individual instructions in written form (individual instruction).

2. Scope and responsibility

seca checks or maintains automated processes or data processing systems on behalf of the client, whereby access to personal data (see Annex 1) cannot be ruled out. This includes actions specified in the Purchase Contract and in the Specifications.

3. Obligations of seca

3.1. seca may collect, process or use data only within the scope of the order in accordance with the Client's documented instructions for the purpose of remote maintenance (Annex 1). Seca shall inform the Client immediately if an instruction violates data protection regulations. In this case, seca is entitled to suspend the execution of the relevant instruction until it has been confirmed or changed by the Client.

3.2. In his area of responsibility, seca will design the in-house organization in such a way that it meets the special data protection requirements. For this purpose, seca will take appropriate technical and organizational measures to ensure adequate protection of the Client's data with regard to their confidentiality, integrity, availability and resilience of the systems. In doing so, seca shall take into account the state of the art, the implementation costs and the type, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR.

A description of these technical and organizational measures can be found in Annex 2) to this Supplementary Agreement. The measures listed there are subject to technical progress and further development. In that regard, seca is allowed to implement alternative adequate measures. In doing so, the safety level of the specified measures may not fall short. Significant changes must be documented.

3.3. seca shall ensure that the employees involved in the processing of the Client's data have been obliged to comply with Art. 28 (3) (2) (b) GDPR and have been instructed in the protection provisions of the Data Protection Regulation. The data secrecy continues even after completion of the activity.

3.4. The contact details for seca's data protection officer are available at: https://www.seca.com/de_de/datenschutz.html

3.5. seca shall inform the Client immediately in the event of serious disruptions to the operation, suspected violations of data protection or other irregularities in the processing of the Client's data.

3.6. seca shall assist the Client in complying with the obligations of securing personal data, reporting data breaches, data protection impact assessment and prior consultation mentioned in Articles 32 to 36 of the GDPR.

All copies or reproductions made of data media remain the property of the Client. seca shall secure these carefully so that they are not accessible to third parties. The Client may request information about this, as far as the personal data and documents of the Client are affected. The data protection-compliant destruction of test and reject material after completion of order processing shall be handled by seca on the basis of an order from the Client. The record of the deletion shall be submitted on request. In special cases to be determined by the Client, there shall be storage or handover. Documentation that serves as proof of the orderly and proper data processing shall be kept by seca according to the respective retention periods beyond the end of the contract. For relief, seca can hand them over to the Client at the end of the contract.

3.7. The fulfillment of the aforementioned obligations shall be checked and evidenced in a suitable manner by seca.

4. Obligations of the Client

4.1. The Parties are responsible for compliance with their respective data protection laws with regard to the personal data to be processed.

4.2. The Client shall inform seca immediately and completely if he/she discover errors or irregularities regarding data protection regulations when checking the order results.

4.3. The Client shall determine the measures for the return of the transferred data media and/or deletion of the stored data after completion of the contract stipulated in the contract or by instruction.

5. Inquiries concerning the Client

5.1. If the Client is obliged to provide information on the collection, processing or use of data to a particular person due to applicable data protection laws, seca shall assist the Client in providing this information. The same applies in the event that an affected person requires the Client to correct, delete or restrict the data processing.

5.2. If a particular person address the Contractor directly to assert his/her rights, the Contractor shall immediately forward this request to the Client.

6. Supervisory duties

6.1. Before taking up the data processing, the Client shall satisfy himself/herself of the scope of protection of the technical and organizational measures taken by seca.

6.2. The Client has the right, in consultation with seca, to carry out checks or have them carried out by examiners appointed in individual cases. He/she has the right to satisfy himself/herself of the observance of this agreement by seca at his/her place of business through random inspections, which shall usually to be announced in good time.

6.3. seca shall ensure that the Client is able to satisfy himself of compliance with the obligations under Art. 28 GDPR. Seca undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence on the implementation of the technical and organizational measures.

7. Sub-contractor

7.1. The forwarding of orders by seca within the context of the activities specified in subsection 2 (1) sentence 2 requires the prior written and documented consent of the Client.

7.2. The Client shall be informed in advance about any further commissioning or replacement of sub-contractors and shall have the option of objecting to the subcontracting of the order.

7.3. In the case of subcontracting, seca is obliged to enter into appropriate and legally compliant contractual agreements and take control measures in order to ensure the data protection and data security of the Client's data, even with outsourced ancillary services. The sub-contractor is also subject to the duties listed under 3.

8. Information obligations, written form clause, choice of law

8.1. Should seca's data be endangered by garnishment or seizure, by bankruptcy or settlement proceedings or by other events or measures by third parties, seca shall immediately inform the Client that the sovereignty and ownership of the data is exclusively at the Client's "Responsible body" within the meaning of the Federal Data Protection Act.

8.2. Changes and additions to this Contract and all of its components - including any warranties made by seca - require a written agreement and an express indication that it is an amendment or supplement to these terms.

8.3. The German law applies. Court of jurisdiction is the headquarters of seca.

Annexes

Annex 1

Additions to paragraph 2 of this order
A. Scope, nature and purpose of the data processing according to Section 2
B. Type of personal data referred to in Section 2
C. Relevant persons in accordance with Section 2

Annex 2
Technical and organizational measures according to Section 3 of this order

Annex 1 to the Contract Data Processing Contract

A. Scope, nature and purpose of data processing according to Section 2
The Contractor shall supervise the Client in the remote support of the Client's seca software for the purpose of remote maintenance. The remote support may include:

- the installation of software (updates)
- troubleshooting software issues related to the user's individual software setup
- maintenance work on the software
- which includes the establishment of integration

software. The processing and use of personal data shall take place exclusively in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another Contracting State to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the Client and may only take place if appropriate protective measures have been taken pursuant to Art. 44 et seq GDPR.

B. Type of personal data according to Section 2
Employee/personnel data ● Employee ID ● Health data ● Patient ID ● Case ID ● Patient data ● Name of the patient ● Gender ● Date of birth ● Ethnicity

C. Circle of the persons concerned according to Section 2
Employees of the client (hospital staff) ● Patients
Annex 2: Technical and organizational measures at seca
Presentation of the technical and organizational measures according to Art. 32 GDPR at seca:

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

1. Access control
No unauthorized access to data processing systems:
Alarm system for sensitive areas (including data processing) ● Transponder locking system ● Lock authorizations via employee-specific locking circuits ● Video surveillance of access ● Protection by motion detectors and light barriers ● Recording of visits from external persons (visitor list and ID cards) ● Careful selection of security and cleaning personnel ● Special security measures for the server rooms

2. Access control
No unauthorized system usage:
Assignment of user rights ● Creation of user profiles ● Authentication with user name/password ● Assignment of user profiles to IT systems ● Use of firewalls with VPN technology ● Use of intrusion detection systems ● Use of central smartphone administration software (for example, for external deletion of data) ● Use of anti-virus software ● Encryption of data media in laptops/notebooks

3. Access control
No unauthorized reading, copying, modification or removal within the system, measures for the demand-oriented design of the authorization concept and the access rights as well as their monitoring and recording:
Differentiated authorizations (profiles, roles, transactions and objects) ● Number of administrators reduced to the "most necessary" ● Password policy including password length, complexity, history, validity ● Recorded system access ● Use of shredders or service providers with a privacy seal ● Specified procedures for approval

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

1. Transfer control
No unauthorized reading, copying, modification or removal during electronic transmission or transport:
Leased line installations or VPN tunnels ● Transmission of data in anonymised or pseudonymised form ● In the case of physical transport: careful selection of transport personnel and vehicles ● Secured wireless LAN ● Data media are irretrievably destroyed or deleted

2. Entry control
Determine if and by whom personal data has been entered, modified or removed from computer systems:
Recording and record evaluation systems ● Comprehensibility of entering, changing and deleting data by means of individual user names (not user groups) ● Assigning rights for entering, changing and deleting data on the basis of an authorization concept

C. Order control:

Clear contract design ● Formalized order placement ● Control of contract execution

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

1. Availability control
Protection against accidental or wilful destruction or loss:
Backup procedures ● Disk mirroring ● Uninterruptible power supply (UPS) ● Separate retention of backups ● Antivirus/firewall ● Emergency plan ● Fire extinguisher and fire alarm system ● Redundant design of the entire infrastructure through multiple data centres ● Air conditioning and monitoring of temperature and humidity in server rooms

2. Rapid recoverability
Regular backups on servers ● Accessibility to backups is always guaranteed

E. Separation control

Separate processing of data collected for different purposes, such as:
Separation of data from different clients ● Separation of functions development/test/production with separate databases

F. Pseudonymisation (Art. 32 (1) (a) of the GDPR, Article 25 (1) of the GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific affected person without the need for additional information, provided that such additional information is kept separate and subject to appropriate technical and organizational measures:

- Internal statement of anonymisation or pseudonymisation of personal data in the case of a transfer or expiry of the deletion period

G. Procedure for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR, Article 25 (1) of the GDPR)

1. Data protection management:
Documented security concept ● external data protection officer ● minimum annual review of the effectiveness of the technical protection measures ● training of employees with regard to the confidentiality of personal data ● commitment of employees to data secrecy ● data protection impact assessment is conducted on a regular basis

2. Incident response management:
Documented process for detection and reporting of security incidents/data breaches ● Documented procedure for dealing with security incidents ● Involvement of the external data protection officer in security incidents and data breaches

3. Privacy-friendly pre-settings (Art. 25 Abs. 2 GDPR):

- Collection of personal data required to achieve the purpose

4. Order control

No order data processing within the meaning of GDPR without corresponding instructions of the client, for example: Clear contract design, formalized order management, strict selection of the service provider, compulsory pre-obligation, follow-up checks, measures (technical, organizational) to delineate the competences between Client and Contractor: Order processing contract that meets the requirements of Art. 28 GDPR