ROLAND CONSULT
Electrophysiology and Imaging

Contract for the Processing of Personal Data

between

Name: ______________________________

____

Address: ______________________________

Postcode / City ______________________________

in the following: **client**

and

Roland Consult Stasche & Finger GmbH
Heidelberger Str. 7
D-14772 Brandenburg, Germany

in the following: **contractor**

- hereinafter referred to individually or collectively as **parties** –

This contract specifies the legal rights and obligations arising for the contracting parties from the applicable data protection law, in particular from the General Data Protection Regulation (VO (EU) 2016/679, hereinafter also "DSGVO") as well as the national data protection laws, in particular the Federal Data Protection Act, if and to the extent that the Contractor processes personal data for the Customer (Annex 1). It shall apply to all activities which are related to the main contract(s) (listed in detail in Annex 1) and during which employees of the Contractor or third parties commissioned by the Contractor may come into contact with personal data of the Customer. Such activities include, in particular, remote access to the Customer's IT system, the handling of a dump / backup file containing real data - especially in connection with support requests - insofar as personal data are contained on the IT system or in the real data. The term of this agreement shall be based on the term of the main contracts. It shall end, without the need for separate termination, at the end of the term of the last remaining main contract listed in Annex 1.

§ 1 Definitions

(1) Personal data: Personal data means any information relating to an identified or identifiable natural person (hereinafter "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(2) Processing: processing includes any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(3) Instruction: Instruction is the documented order of the Customer directed at a specific data protection handling (for example anonymization, blocking, deletion, surrender) of the Contractor with personal data. The instructions are initially defined by the main contract and can subsequently be changed, supplemented or replaced by the Customer in documented form by individual instructions (individual instruction).

§ 2 Scope of application

(1) The Contractor shall test and maintain automated processes or data processing systems on behalf of the Customer, in particular the standard software provided by the Contractor under a separate contractual relationship, and shall offer further assistance in the use of the software within the scope of its support services. Within the scope of these activities, access to personal data cannot be excluded in special constellations. The activities covered are specified in the service description of the main contract. The main contracts are also listed in Annex 1 to this Agreement, with a reference to the categories of data concerned in each case. The list shall be updated by the parties on an ongoing basis in the event of the discontinuation or conclusion of a new main contract which also covers commissioned processing.

(2) The rights and obligations imposed on the parties under this Agreement shall only apply during the term of the Agreement and within this period only during the periods in which commissioned processing is actually carried out or a comparable risk situation exists for personal data for which the Principal is the Controller.

§ 3 Obligations of the Contractor

(1) The Contractor may only process personal data within the scope of the order and the documented instructions of the Customer. In addition, a legal obligation to process personal data may arise for the Contractor in individual cases. In this case, the Contractor shall notify the Customer of these legal requirements prior to processing, unless the relevant legal obligation prohibits such notification due to important public interest.

(2) The Contractor shall organize the internal organization within its area of responsibility in such a way that it meets the special requirements of the applicable data protection law. It shall take the appropriate and legally required technical and organizational measures to ensure a level of protection appropriate to the risk. This includes in particular

- the encryption of personal data;
- the ability to ensure the confidentiality, integrity, availability and resilience of the systems and services related to the processing on a permanent basis;
- the ability to rapidly restore the availability of and access to personal data in the event of a physical or technical incident;
- A procedure for periodically reviewing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the security of the processing.

A description of these technical and organizational measures shall be attached as an appendix to this Agreement.

(3) The Contractor shall ensure that the persons authorized to process the Personal Data have committed themselves to confidentiality or are subject to an appropriate legal confidentiality obligation.

(4) The Contractor has appointed a company data protection officer and shall inform the Customer of the contact details of the company data protection officer.

(5) The Contractor shall support the Customer in complying with the obligations set out in Art. 32 to 36 DS-GVO regarding the security of personal data, notification obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes, among other things.

- ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential security breach and allow for immediate detection of relevant breach events;
- the obligation to report personal data breaches to the Principal without undue delay;
- the obligation to support the Principal in its duty to inform the Data Subject and to provide it with all relevant information in this context without undue delay;
- the appropriate support of the principal for its data protection impact assessment; and
- the appropriate support of the Customer in the context of prior consultations with the supervisory authority.

The Customer shall reimburse the Contractor for any costs and expenses incurred as a result of the support. If the Parties cannot agree on the scope of reimbursement, the costs that the Contractor was entitled to consider necessary shall be reimbursed in full.

(6) Data carriers provided as well as all copies or reproductions made thereof shall remain the property of the Customer. The Contractor shall store them carefully so that they are not accessible to third

parties. The Contractor shall undertake the destruction of test and reject material in compliance with data protection requirements on the basis of an individual order by the Customer. In special cases to be determined by the Customer, storage or handover shall take place.

(7) The Contractor shall monitor the fulfillment of the aforementioned obligations and provide appropriate evidence upon request.

(8) The commissioned processing may only take place within the territory of a Member State of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country outside this territory shall require the prior consent of the Principal.

§ 4 Obligations of the Customer

(1) The Customer shall be responsible for the processing of data on behalf of the Contractor within the meaning of the applicable data protection law (responsible party). The assessment of the permissibility of the data processing shall be incumbent upon the Customer.

(2) The Customer shall have the right to issue supplementary instructions to the Contractor at any time regarding the purpose, type and scope of the processing of data (individual instructions). The Customer shall bear any additional costs incurred as a result; the Contractor may demand an advance payment. The Contractor may refuse to carry out additional or modified data processing if it would lead to a significant change in the workload or if the Customer refuses to reimburse the additional costs or the advance payment.

(3) As the responsible party, the Client shall be responsible for safeguarding the rights of the data subjects. Should third parties assert claims against the Contractor on the basis of allegedly unlawful data processing, the Customer shall, insofar as such allegedly unlawful processing is based on intent or negligence on the part of the Customer, indemnify the Contractor against all such claims upon first request. Insofar as the Contractor supports the Customer in fulfilling the claims of data subjects (in particular with regard to correction, deletion and blocking of data), the Customer shall reimburse the Contractor for costs and expenses. The parties shall agree on the expected scope of costs and effort.

(4) The Customer shall inform the Contractor immediately and in full if it discovers errors or irregularities with regard to data protection provisions when checking the results of the order.

§ 5 Control Duties

(1) The Customer shall convince itself of the technical and organizational measures of the Contractor prior to the commencement of data processing and regularly thereafter and document the result. The information required for this purpose shall be made available to the Customer in accordance with the following paragraph.

(2) The Contractor shall provide the Customer with all information necessary to prove compliance with the obligations regulated in this Agreement. He shall enable and contribute to checks - including inspections - carried out by the Customer or another inspector appointed by the Customer.

(3) The frequency of inspections shall be no more than once a year. This shall be without prejudice to the right of the Customer to carry out further inspections on an ad hoc basis in the event of violations of data protection obligations by the Contractor.

(4) At the Contractor's discretion, proof of compliance with the technical and organizational measures may be provided by submitting a suitable attestation, reports or report excerpts from independent bodies (e.g. auditor, auditor, internal or external data protection officer, IT security department, data protection auditor, quality auditor) or a suitable data protection certification by an approved body ("certification certificate") instead of an on-site inspection. The Certification Document must enable the Customer in a reasonable manner to satisfy itself of compliance with the technical and organizational measures in accordance with the enclosed Annex.

§ 6 Subcontractors

(1) The Customer agrees that the Contractor may engage the additional order processors (subcontractors) named in the Annex in order to fulfill its contractually agreed services. The Contractor shall inform the Customer of any changes to the subcontractors named in the Annex and give the Customer the opportunity to object to such changes.

(2) In all other respects, the commissioning of subcontractors by the Contractor shall only be permissible with the prior consent of the Customer. Such consent may only be refused for good cause to be proven to the Contractor.

(3) The Contractor has contractually imposed the same obligations on the Processors named in the Annex as under this Agreement and shall impose the same obligations on further Processors, including sufficient guarantees that the appropriate technical and organizational measures will be implemented in such a way that the Processing will be carried out in accordance with the statutory requirements. By written request, the Customer shall be entitled to obtain information from the Contractor about the essential content of the contract and the implementation of the subcontractor's data protection-related obligations, if necessary also by inspecting the relevant, data protection-related contractual documents.

§ 7 Information Duties

(1) Should the Customer's data at the Contractor be endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Customer thereof without undue delay. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Customer as the "responsible party" within the meaning of the applicable data protection law.

§ 8 Term and Termination of the Agreement

(1) The term of this Agreement shall correspond to the term of the last existing main contract.

(2) Upon completion of the provision of the Processing Activities or upon termination of the Agreement, the Contractor shall, at the option of the Customer, delete or surrender all Personal Data.

This shall not apply if the Contractor has an obligation to store the personal data on the basis of the applicable data protection law (e.g. statutory retention obligation).

(3) The Customer shall determine the measures for the return of the data carriers provided and / or deletion of the stored data after termination of the order by contract or by instruction. Any additional costs resulting from the return or deletion of the data shall be borne by the Client.

§ 9 Final Provisions

(1) The parties agree to mutually adapt and amend the present contract including annexes in the event of changes, adaptations and / or additions to data protection regulations - in particular the DSGVO and / or the respective national data protection laws.

(2) Amendments and supplements to this Annex and all its components - including any warranties of the Contractor - shall require a written agreement and the express indication that it is an amendment or supplement to these Terms and Conditions. This shall also apply to any waiver of this formal requirement.

(3) This Agreement shall be governed by the laws of the Federal Republic of Germany to the exclusion of the UN Convention on Contracts for the International Sale of Goods and the conflict of laws rules. The exclusive place of jurisdiction is Frankfurt (Oder).

(4) Should individual parts of this contract be invalid, this shall not affect the validity of the remaining provisions of the contract.

City, Date, ____________________

Brandenburg, 2.12.2021

____
Client

____
Contractor (Roland Consult Stasche&Finger GmbH)

Roland Consult
Stasche & Finger GmbH
Heidelberger Straße 7
14772 Brandenburg an der Havel
Tel.: 03381-890 1034
Fax: 03381-890 2994

Annex 1: Software products

Please check	Main contract	Affected data categories and persons	Subcontractor employed / location of data processing
☒	Software Team Viewer for Remote Control and Monitoring Device: RETI-port/scan 21	Patient data, examination data	-
☒	Service at device RETI-port/scan 21 in examination rooms	Patient data, examination data	-
☒	Service at device RETI-port/scan 21 at Roland Consult Stasche & Finger GmbH	Patient data, examination data	-

Appendix 1: Technical and Organizational Measures (TOM) according to Art. 32 GDPR

concerning software maintenance services of Roland Consult Stasche & Finger GmbH
(i.e., accesses to software troubleshooting and remote support)
as of: May 15, 2021

Organizations that collect, process or use personally identifiable information, whether on their behalf or on their behalf, must take the technical and organizational measures necessary to ensure that the privacy laws are enforced. Measures are only required if their effort is proportionate to the intended purpose of protection.

1. Confidentiality acc. Art. 32 para. 1 lit. GDPR

1.1 Access control
Visitors must register at the reception, their identity is checked and they are only allowed to enter the premises when accompanied. Access to the server room is only possible for selected employees. All premises are secured outside working hours by means of an alarm system. A watchful alert is given.

1.2 Access control
To log in to the network requires a password with a given minimum length. You should use numbers and special characters, as well as uppercase and lowercase letters. In certain constellations, a 2-factor authentication is required.
An automatic blocking of the user takes place after three incorrect entries during the user logon. Activation of the screen saver takes place automatically after 5 or 10 minutes and can only be released again via password input.
User authentication is mapped using a central directory service. Basically and as far as not technically necessary, access to order data is only permitted by means of personalized accounts.
The system is constantly monitored by a firewall. There is antivirus software at the system level. In addition, the antivirus software for each client and server is installed for the mail system. Only IT systems are used, which are supported by the manufacturer through regular security updates.

1.3 Access Control
Access control is set up at the user level.

1.4 Separation control
As far as a separate processing and evaluation of the databases is required, this will be set up accordingly. There are also own test environments.

1.5 Pseudonymisation (Article 32 (1) (a) GDPR, Article 25 (1) GDPR)
Not considered an option for software maintenance services.

2. Integrity (Article 32 (1) (b) GDPR)

2.1 Transfer Control
Connections to networks are made exclusively via VPN and corresponding remote software. Accesses and requests are logged here.

2.2 Input control
All network logon and logoffs as well as all transactions (e.g., new installations, changes, deletions) are logged.

3. Availability and resilience (Article 32 (1) (b) GDPR)

3.1 Availability control

A weekly backup (full backup) is performed. In addition, daily incremental backup is provided. A RAID procedure is used for the hard disk backups. Uninterruptible power supply (UPS) with overvoltage protection is available. Through the use of the firewall and the antivirus software for the mail system and all servers, as well as antivirus software per client, the best possible technical availability is ensured.

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

4.1 Privacy Management

All employees at Roland Consult Stasche & Finger GmbH are committed to data secrecy. There is a regular instruction of the employees in the data protection. A privacy policy has been created. An external data protection officer has been appointed: Prof. Dr. Reiner Creutzburg, E-Mail: rcreutzburg@web.de. The organization complies with the information obligations under Art. 13 and 14 GDPR. The effectiveness of our technical protective measures is checked regularly.

4.2 Incident Response Management

Firewalls, spam filters and virus scanners are used and regularly updated. There are also systems for intrusion detection and prevention. A policy regulates the handling of security incidents. There are alarm plans and documentation of security incidents and data breaches. The data protection officer, the security officer and the legal department are always involved. In coordination with the data protection officer, the notification is sent to the supervisory authorities.

4.3 Privacy-friendly default settings (Article 25 (2) GDPR)

The processes for software maintenance services that are related to personal data are clearly defined and the employees involved are obliged to do so by binding work instructions. This includes that customer data can only be received and managed via the data safe. Employees are required to collect no more personally identifiable information than is necessary for their purpose.

4.3 Order control (outsourcing to third parties)

Our employees know the data processing purpose. You receive instructions for handling personal data. Special subcontracting conditions (subcontractors) are mandated in writing and are listed in the respective products or services in Appendix 1.