Supplementary Agreements to the General User Agreements - Order Processing pursuant to Art. 28 (3) DSGVO

between

User according to CNXT User Agreement

hereinafter referred to as **"customer"**

and

Rodenstock GmbH
Elsenheimerstr. 33
80687 Munich

hereinafter referred to as **"Rodenstock"**

Preamble

Rodenstock comes into contact with personal data when providing its services for the customer. This agreement establishes rules which guarantee that Rodenstock handles data carefully, thus ensuring a high data protection standard is maintained in the customer's company and Rodenstock.

§ 1 Subject matter of the contract and scope

A contractual relationship exists between the customer and Rodenstock. This order processing contract including all annexes (hereinafter referred to jointly as **agreement**) provides details of the data protection obligations of the parties from the underlying contract, the performance agreement and/or order description including all annexes (hereinafter referred to jointly as **contract**). This agreement applies to **all services** for which the customer transfers personal data to Rodenstock required for the execution of the respective order for the duration of the order processing or for which Rodenstock may process or access personal data. The contract, as well as components of the contract, are published on the CNXT website under the section "Trust Centre" and can be viewed there at any time.

§ 2 Scope, nature and purpose of data collection, processing or use

The subject matter of the contract is all services which Rodenstock provides to the customer. The services may cover the following activities and objectives, among other things:

Availability of the CNXT portal for the following purposes:

- Networking of different optical or medical measuring instruments with various end devices (PCs, tablets, etc.) for the purpose of data exchange.
- Reduction of administrative and manual activities in relation to data collection for lens consultation and/or order.
- Merging and saving of all recorded customer and measurement data in order to make it available on all connected devices.
- The data can be edited via the CNXT user interface.
- Evaluation of the data for the purpose of optimisation and further development of our products, as well as the development of new services.

Apart from that, the scope, nature and purpose of the collection, processing or use of personal data by Rodenstock stem from the underlying user contract. Rodenstock shall process the personal data which is used within the framework of the aforementioned services. The data may include:

- Data of the customer (user), e.g. title, surname, first name, company, address details, e-mail address, telephone and fax numbers, role
- Client data of the customer, e.g. title, surname, first name, sex, addresses, e-mail address, telephone number, health records (incl. photos of ocular fundus, analytical reports, comments).

The agreement shall end automatically upon termination of the business relationship or at the end of the user contract.

§ 3 Rights and obligations of the customer

(1) The customer shall be solely responsible for the assessment of the reliability of the data processing as well as for safeguarding the rights of the data subjects and thus for the processing by the controller pursuant to Art. 4(7) GDPR.

(2) The customer shall be entitled to issue instructions about the nature, scope and method of data processing. At the request of the customer, oral instructions shall be confirmed immediately by Rodenstock in writing or in text form (e.g. by e-mail).

(3) Individuals authorised to issue instructions may be appointed to the extent deemed necessary by the customer. The customer shall notify Rodenstock thereof in writing or in text form. If there are any changes to these individuals authorised to issue instructions for the customer, Rodenstock shall be notified thereof in writing or in text form with designation of the new individual.

(4) The customer shall immediately inform Rodenstock of any errors or irregularities identified in connection with the processing of personal data by Rodenstock.

§ 4

Duties of Rodenstock

(1) Data processing

Rodenstock shall only process personal data according to this agreement and/or the underlying main contract as well as in accordance with the instructions of the customer.

(2) Rights of the parties concerned

a. Rodenstock shall support the customer to the extent possible with the fulfilment of the rights of the parties concerned, particularly with regard to correction, restriction of the processing and deletion, notification and exchange of information. If Rodenstock processes the personal data mentioned in § 2 of this agreement on behalf of the customer and if this data is the subject matter of a request for data portability in accordance with Art. 20 GDPR, Rodenstock shall make available the respective data record to the customer within a reasonable time, otherwise seven working days, in a structured, standard and machine-readable format.

b. On instruction of the customer Rodenstock shall correct, delete or restrict the processing of the data mentioned in § 2 of this agreement, which is processed in the order. The same shall apply if this agreement provides for a correction, deletion or restriction of the processing of data.

c. Insofar as a data subject contacts Rodenstock directly for the purpose of correction, deletion or restriction of the processing of the data mentioned in § 2 of this agreement, Rodenstock shall forward this request to the customer immediately upon receipt.

(3) Control obligations

a. Rodenstock shall ensure through appropriate inspections and checks that the personal data processed in the order is processed solely according to this agreement and/or the main contract and/or the corresponding instructions.

b. Rodenstock shall organise its company and operations so that the data which it processes on behalf of the customer is secured to the extent required and protected against unauthorised access by third parties.

c. Rodenstock shall confirm, according to Art. 37 GDPR and, to the extent applicable, according to § 38 German Federal Data Protection Act (BDSG), that a data protection officer has been appointed and compliance with the regulations on data protection and data security is monitored with full involvement of the data protection officer. Our data protection officer can be reached as follows:

Rodenstock GmbH
FAO Data Protection Officer
Elsenheimerstr. 33
80687 Munich

E-mail: datenschutz@rodenstock.com

(4) Obligations to provide information

a. Rodenstock shall immediately alert the customer if in its opinion an instruction issued by the customer infringes statutory provisions. Rodenstock shall be entitled to defer the implementation of the corresponding instruction until it is confirmed or modified by the customer.

b. Rodenstock shall support the customer in meeting the obligations stated in Articles 32 to 36 GDPR taking into consideration the nature of the processing and the information in its possession.

(5) Place of data processing

The data is generally processed in the area of the Federal Republic of Germany, in a member state of the European Union or in another signatory state to the European Economic Area. Each relocation to a third country shall only take place if the special requirements of Art. 44 ff. GDPR are fulfilled.

(6) Deleting personal data after completion of the order

After termination of the main contract Rodenstock shall at the discretion of the customer either delete or return all personal data processed in the order insofar as the deletion of this data does not conflict with any statutory retention requirements of Rodenstock. The deletion protected by data protection regulations shall be documented and confirmed to the customer on request.

§ 5 Monitoring rights of the customer

(1) The customer shall be entitled to check at its own expense compliance with the regulations on data protection and the contractual agreements to the required extent either itself or through a third party, after timely prior notification during the normal business hours

without interrupting the business operations of Rodenstock or jeopardising the security measures for other customers. The inspections may also be carried out by accessing existing certifications of the Rodenstock company, current certificates or reports from an independent body (e.g. auditor, external data protection officer, external auditor or external data protection auditor) or self-declarations. Rodenstock shall offer the necessary assistance for the implementation of the inspections.

(2) Rodenstock shall inform the customer about the execution of control measures of supervisory authorities if the measures or data processing may affect what Rodenstock provides for the customer.

§ 6 Subcontracting

(1) The customer shall authorise Rodenstock to make use of other companies according to the following sections in § 6 of this agreement. This authorisation shall represent general written consent pursuant to Art. 28(2) GDPR.

(2) For the fulfilment of the contract Rodenstock is currently working with the subcontractors listed in **Annex 2**. The customer has agreed to their commissioning.

(3) Rodenstock shall be entitled to commission other companies or replace those companies already appointed. Rodenstock shall inform the customer in advance about each planned change in relation to the addition or replacement of another company. The customer may raise an objection to a planned change.

(4) The objection against the planned change shall be raised with Rodenstock within 2 weeks of receipt of the information about the change. In the event of an objection, Rodenstock may at its discretion provide the service without the intended change or – if the provision of the service without the intended change is not acceptable to the company, e.g. due to associated disproportionate expenses for Rodenstock – terminate this agreement as well as the main contract without observing a period of notice.

(5) With the involvement of another company a level of protection that is comparable with that of this agreement must always be guaranteed. Rodenstock shall be responsible to the customer for all the actions and failures of the other companies it employs.

§ 7 Confidentiality

(1) Rodenstock is obligated to maintain confidentiality when processing data for the customer.

(3) Rodenstock undertakes to only employ staff or other vicarious agents for the execution of the order, who are committed to maintain confidentiality in handling personal data and have been made aware of the data protection requirements in an appropriate manner. Rodenstock shall prove the implementation of the obligations to the customer upon request.

(4) If the customer is subject to any other secrecy regulations, it shall inform Rodenstock thereof. Rodenstock shall commit its employees to these secrecy regulations according to the requirements of the customer.

§ 8 Technical and organisational measures

(1) The technical and organisational measures described in **Annex 1** are agreed as appropriate. Rodenstock may update and change these measures, provided that the level of protection is not substantially reduced by such updates and/or changes.

(2) Rodenstock observes the principles of proper data processing according to Art 32 in conjunction with Art. 5(1) GDPR. Rodenstock shall guarantee the contractually agreed and statutory data security measures. Rodenstock shall adopt all necessary measures for the safeguarding of the data or the security of the processing, particularly also considering the state of technology, as well as to mitigate possible negative effects for parties concerned. The measures to be adopted include measures for the protection of confidentiality, integrity, availability and capacity of the systems and measures that ensure the continuity of the processing after incidents. In order to be able to always ensure an appropriate security level for processing, Rodenstock shall regularly evaluate the implemented measures and make any necessary adaptations.

§ 9 Liability/Exemption

(1) According to statutory regulations, Rodenstock shall be liable to the customer for all damage due to culpable breaches of this agreement as well as the statutory data protection regulations appropriate to Rodenstock, which Rodenstock, its employees or the representatives appointed by it for the execution of the contract cause in the performance of the contractual services. Rodenstock shall not be obligated to pay compensation if Rodenstock proves that the data of the customer it received was processed solely according to the instructions of the customer and it fulfilled its GDPR obligations incumbent on Rodenstock.

(2) The customer shall exempt Rodenstock from all claims by third parties, which are asserted against Rodenstock based on a culpable breach of the obligations from this agreement or applicable data protection regulations by the customer.

§ 10 Other

(1) In the event of conflict between the provisions in this agreement and the provisions of the main contract, the provisions of this agreement shall take precedence.

(2) Any changes and supplements to this agreement require the mutual consent of the contracting parties with reference to the provision of this agreement to be changed. Oral agreements do not exist and are also excluded for future changes to this agreement.

(3) This agreement is subject to the law of the state in which Rodenstock has its registered office.

(4) The registered office of Rodenstock is the sole and international place of jurisdiction for merchants in terms of commercial law, public law entities or special funds under public law.

(5) Rodenstock shall immediately notify the customer if access to the data which the customer transferred to Rodenstock for data processing is jeopardised by third party measures (e.g. measures of an insolvency administrator, seizure by financial authorities, etc.).

_____	_____
Town/City, Date	Town/City, Date
_____	_____
Signature (customer)	Signature (Rodenstock)

Schedule of Annexes

Annex 1 Technical and organisational measures of Rodenstock for ensuring the security of the data processing

Annex 2 Subcontracting acc. to § 6 of the Agreement on Order Processing

Annex 1

Technical and organisational measures for ensuring the security of the data processing

Rodenstock assures that it has taken the following technical and organisational measures:

A. Measures for pseudonymisation

Measures which reduce the direct personal reference during processing in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. The additional information shall be kept separately to the pseudonym and is subject to technical and organisational measures.

Description of the pseudonymisation:

- Pseudonymisation of personal data within the framework of market research

B. Encryption measures

Measures or methods where a plain readable text / information is converted into an unreadable format, i.e. character strings cannot be easily interpreted (ciphertext), by means of an encryption system (crypto system):

- Client VPN encryption TLS> 1.1
- Site2Site VPN encryption AES256, 3DES
- Websites with user login are encrypted using TLS
- Encrypted password storage in central system

C. Measures for protecting confidentiality

1. Access control

Measures which physically deny unauthorised individuals from accessing IT systems and data processing systems with which personal data is processed, as well as confidential files and data carriers:

Description of the access control system:

- PCs are locked upon leaving the workstation.
- The validity of accounts of external employees is limited to 12 months.
- Door protection (electronic door opener, etc.)
- Premises security/doorman
- Monitoring equipment (alarm systems)
- Secure server room
- Control system for visitors
- Company telephones are protected by MDM (Mobile Device Management)

• Access to company premises: fence, turnstile, barrier
• Access to company building: chip card, badge reader, controlled key assignment,
• Access to data centre by external service providers ISAE3402
• Access to server room: chip card only for selected employees
• Access to data backup only by authorised individuals (access-controlled area)
• Premises protection on all days (incl. weekend)
• Monitoring of premises by video recording

2. **Access control**

Measures which prevent unauthorised individuals being able to process or use data protected by data protection regulations.

Description of the access control system:

• Access routes are SSL or AES256 encrypted
• Directory service (Active Directory)
• Regularly updated anti-virus and spyware filter
• Rights management system: limit of the number of authorised employees
• Firewall and UTM appliances
• Guest WLAN protected with voucher.
• Employee / Equipment WLAN protected with Personal Security Key (PSK)
• Anti-virus protection is installed at the time the computer is installed and updated regularly.

3. **Access control**

Measures which ensure that the individuals authorised to use the data processing method only access the personal data based on their access right so that data cannot be read, copied, changed or removed by unauthorised individuals during processing, use and storage.

Description of the access control system:

• User accounts and role changes are requested by the department. The check is carried out by the cost centre manager, the implementation by IT administrators.
• Windows Active Directory Server: central assignment of rights at the respective site by IT staff
• It gives the instruction to all staff to check the USB stick for malware before using USB sticks.
• Access to data backup only by authorised individuals (access-controlled area)
• Authorisation requests via SharePoint with approval workflow

4. Separation rule

Measures which ensure that data collected for different purposes is processed separately and thus separately from other data and systems so that unplanned use of this data for other purposes is ruled out.

Description of the separation control process:

• Activity-specific roles for file access

• The individual systems (SAP/Fileserver/DB) are installed on separate systems
• Separation of test and productive systems
• Authorisation concepts

D. Measures for safeguarding integrity

1. Data integrity

Measures which ensure that stored personal data is not damaged by system malfunctions:

General description of data integrity:

• Function test upon installation and releases/patches by IT Department
• In SAP there is a controlled transport process using the dual control principle
The importing of releases and patches is carried out in SAP with the ticket system SAP Solution Manager. There is always an installation in the test systems first. Together with key users tests are carried out before a productive installation. The dual control principle is guaranteed.
• Client and Server Patch Management on Microsoft systems is performed using MS-WSUS. For the production areas first test groups in IT and individual users in departments are supplied with patches and a test operation is carried out lasting several weeks. Only then is there a comprehensive roll-out.
• SAP and DB patches are patched regularly by the admins based on notifications from the manufacturer. The roll-out always takes place initially on the test systems. Together with key users tests are carried out before a productive installation.

Additional measures, solely for CNXT:

• During the entire life cycle (concept, development, maintenance, decommissioning), quality assurance is carried out according to the rules of the Computerized System Validation (CSV).
• The quality management of Rodenstock has issued a process instruction for CSV and monitors its compliance.
• The safeguarding of data integrity is a central concern of the CSV methodology.

Special features of the process instruction:

- Documentation
  Requirements, risks, test specifications, test results, architecture, installations and updates are documented in writing and are tamper-proof.
- Processes
  Defined processes and responsibilities for new development and maintenance tasks.
- Risk
  All functions concerning the data integrity are subjected to a risk assessment, depending on the risk regarding data integrity safeguarding measures are adopted.

2. Transfer control

Measures which ensure that it is possible to verify and establish to which bodies personal data has been or may be transmitted or made available using data communication equipment:

Description of the transfer control:

• Logging

• User authorisation for the respective systems

3. Transport control

Measures which ensure that the confidentiality and integrity of the data is protected during the transfer of personal data as well as transport of data carriers:

Description of transport control:

• VPN tunnel within the company group (MPLS)
• Access to data backup only by authorised individuals (access-controlled area)
• Transport processes with individual responsibility
• Encryption processes which detect data changes during transport

4. Input control

Measures which ensure that it is subsequently possible to verify and establish whether personal data has been input into automated data processing systems, modified or removed and by whom.

Description of the input control process:

• Logging of all system activities and retention of these logs (SAP system)
• Change documents in the SAP HCM system

Special feature of the input control process for CNXT:

• The data in CNXT is entered, changed or removed by the customer.
• The customer uses CNXT by means of their access control.

E. Measures for securing the availability and capacity

1. **Availability control**

Measures which ensure that personal data is protected against accidental destruction or loss.

Description of the availability control system:

• Important services are generally designed redundantly. This also applies to HW Raid disk systems.
• Important systems are divided between separate data centres.
• Redundant UPS with redundant sub-distributions available in both data centres
• Emergency power diesel systems available in both data centres
• Fire alarm system available in both data centres
• Gas extinguishing system available in both data centres
• Redundant air-conditioning of data centres also in the event of a power failure

- Virtualized systems with VMWare
- Special access protection in the data centres and for tape security and the safes
- Monitoring of critical systems
- SAP high-availability databases
- IBM data centre divided into 2 data centre sites

2. Rapid recovery

Measures which ensure the ability to rapidly restore the availability of personal data and access to the data in the event of a physical or technical incident.

Description of the measures for rapid recovery:

- Emergency plan incl. emergency manual
- Data backup procedure
- Regular tests of data recovery by new setup of test systems (SAP)
- Virtualized systems with VMWare
- SAP high-availability databases (IBM redundant at two sites)

3. Reliability

Measures which ensure that all system functions are available and any malfunctions are reported:

Description of the reliability measures:

- Automatic monitoring with e-mail notification
- Emergency plans with responsibilities
- IT emergency on-call service

F. Measures for the regular evaluation of the security of data processing

1. Verification procedure

Measures which ensure secure processing in compliance with data protection regulations.

Description of the verification procedure:

- Data protection management
- Formal processes for data privacy incidents
- Annual IT check by external auditor
- Data Protection Officer
- Data Protection Officer, IT Manager and managers informed about data privacy incidents
- Regular maintenance of technical equipment / maintenance contracts
- Test runs of emergency diesel power

2. Order control

Measures which ensure that personal data processed in the order can only be processed according to the instructions of the customer:

Description of the order control measures:

- Instructions of the customer are documented (see OPC)

Annex 2

Subcontracting acc. to § 6 of the Agreement on Order Processing

For the fulfilment of the contract Rodenstock is currently working with the following other companies. The customer has agreed to their commissioning.

1. SpaceNet AG, Joseph-Dollinger-Bogen 14, 80807 Munich,
Services: Operator of external computer centre services
2. EasyScan GmbH, Kasinostrasse 19-21, D-42103 Wuppertal,
Services: Supply, installation and support of the Rodenstock FundusScanner
3. ARS Computer und Consulting GmbH, Garmischer Strasse 7, 80339 Munich,
   Services: Support in the backend maintenance and development area.
4. freed Interactive BV, Lauwersweg 9, 9231 GR Surhuisterveen Achtkarspelen, Friesland
   Services: Support in the frontend maintenance and development area.