Data processing contract

between

_____

_____

_____

- Customer -

and

Schenck RoTec GmbH
Landwehrstraße 55
64293 Darmstadt
Germany

- Contractor -

The Customer operates a machine, system and/or a software product that has been supplied by the Contractor. For the purpose of carrying out commissioning and service activities on machines, systems and/or software products of the Customer, the Contractor will also use online remote access and/or remote maintenance via a protected Internet connection insofar as there is an appropriate reason for effective performance.

With regard to the remote access connection to the Customer's machine, system and/or software product, the possibility that employees of the Contractor may also become aware of personal data stored on the machine, system and/or software product by employees of the Customer cannot be ruled out entirely.

The parties therefore agree on a data processing agreement as per GDPR Article 28.

Irrespective of this data protection agreement, every business transaction involving online remote access to machines, systems and/or software products requires the explicit approval of the Customer.

1. General

(1) The Contractor processes personal data on behalf of the Customer and in accordance with the instructions of the Customer. The Customer is responsible for such data within the meaning of data protection regulations ("**Customer Data**").

Insofar as reference is made to "**data processing**", "**handling**" or "**processing**" (of Customer Data) in this contract, such a reference generally refers to the use of personal data. The "**use**" of Customer Data specifically includes the collection, storage, transmission, blocking, erasure, anonymisation, pseudonymisation, encryption or any other use of Customer Data.

(2) The following types/categories of data are the subject of personal data processing:

Data that could be stored by the Customer's employees on machines, systems and/or in software products, which could also contain personal information.

2. Subject of the order, site of data processing

(1) The order given to the Contractor by the Customer includes the services and/or the obligations within the scope of liability for defects arising from the main contract. Such services and obligations are described in greater detail in the main contract. Depending on the type and content of the data that could be stored on the machine, system and/or software products, the circle of data subjects affected by data processing includes:

- Employees of the Customer
- Clients of the Customer
- Suppliers of the Customer

(2) The processing of Customer Data by the Contractor is carried out exclusively in member states of the European Union or in a state party to the Agreement on the European Economic Area (EEA). Any use of data outside the aforementioned area, including by way of granting access to Customer Data to persons outside the aforementioned area, requires the prior written consent of the Customer. Data may only be used in countries that are neither member states of the European Union nor contracting parties of the EEA ("**third countries**") subject to the further condition that the requirements of GDPR Article 44(ff) are met to the satisfaction of the Customer.

(3) The Contractor does not acquire any rights to Customer Data.

3. Rights and obligations of the Customer

(1) The Customer is the Data Controller (GDPR Article 4(7)) for the processing of Customer Data by the Contractor.

(2) The Customer is responsible externally, i.e. vis-à-vis third parties and data subjects, for safeguarding the rights of data subjects in accordance with GDPR Article 15(ff). The rights of data subjects are therefore to be asserted against the Customer.

(3) The Customer is the owner of Customer Data and, in terms of the relationship between the parties, the Customer is the owner of all possible rights to Customer Data.

(4) In the event that there is an obligation to inform third parties, for example under GDPR Article 34, the Customer is responsible for the fulfilment of any such obligations.

4. Obligations of the Contractor, data security

(1) The Contractor processes Customer Data solely within the scope of the agreements made and in accordance with the instructions of the Customer. In doing so, the Contractor complies with the statutory obligations imposed on them by the GDPR. The Contractor is forbidden from carrying out any processing that deviates from these obligations unless the Customer has agreed to such processing in writing.

(2) The Contractor is not permitted to make any copies or duplicates of Customer Data without the prior written consent of the Customer, unless and to the extent that such copies or duplicates are necessary to ensure proper data processing or to ensure compliance with statutory storage obligations. Furthermore, the Contractor is not permitted to transfer Customer Data to third parties or other recipients without the prior written consent of the Customer. This does not apply to the transfer of data to subcontractors who have been commissioned with the Customer's consent in accordance with section 6.1.

(3) The Contractor will label the data which they process on behalf of the Customer in an appropriate manner and keep such data separate from other data stocks.

(4) Insofar as data is processed for different purposes, the Contractor will label such data according to the respective purpose.

(5) If requested to do so, the Contractor is to provide the Customer with an up-to-date list in accordance with GDPR Article 30(2) and 30(3).

(6) The Contractor confirms that they have appointed a company data protection officer within the meaning of GDPR Article 37 and that said data protection officer will carry out their activities in accordance with GDPR Article 38 and 39. The data protection officer can be reached at SCHENCK RoTec GmbH, Landwehrstrasse 55, 64293 Darmstadt, Germany, phone no. +49 6151 32-0, or at dataprotection@schenck.net. The Contractor is obligated to ensure that a company data protection officer is appointed for the term of the contract. The Customer is to notify the Contractor in writing if there is a change of data protection officer.

(7) The Contractor is obligated to design their business and operating procedures in such a way that Customer Data is secured to the extent necessary in each case and protected from unauthorised access by third parties. The Contractor will inform the Customer, in a timely advance manner, of any changes in the organisation of data processing on behalf of the Customer insofar as such changes are relevant to the security of the data.

(8) The Contractor is obligated to notify the Customer of any violation of data protection regulations or of the contractual agreements made and/or the instructions given by the Customer. This obligation relates to any violation that has occurred in the course of data processing by the Contractor or other parties involved in the processing.

(9) In the event that the Contractor discovers or comes to the assumption that

- special types of personal data (GDPR Article 9) or
- personal data relating to criminal offences or administrative offences (GDPR Article 10)

that they have processed for the Customer have been unlawfully transmitted or otherwise unlawfully come to the knowledge of third parties or data processing operations are carried out which require a data protection impact assessment, the Contractor is to notify the Customer in writing or electronic form (fax/e-mail) no later than on the following working day. Notification is to include the time, nature and scope of the transmission. In addition, the Contractor is also obligated to give notification of the measures taken by the Contractor to prevent such transmissions from occurring in the future, insofar as this is within their area of responsibility and does not require instructions from the Customer as per section 5 (1).

(10) The Contractor is obligated to notify the Customer of any violation of the protection of personal data no later than the following working day and to assist the Customer – at first request – with their awareness-raising, remedial and information measures in this respect, including all actions taken to fulfil statutory obligations, within reasonable limits and in accordance with the contractual agreements between the parties. In particular, the Contractor will immediately take all reasonable measures to minimise and eliminate the resulting threats to the integrity or confidentiality of Customer Data, to secure Customer Data and to prevent potential negative consequences for data subjects or to limit their effects as far as possible.

5. Scope of the authority to issue instructions

(1) The Customer confirms oral instructions without delay (in text form as a minimum requirement). The Contractor may assume that persons who issue instructions to them are also entitled to issue such instructions.

(2) The Customer has the right to issue supplementary instructions regarding the type and scope of data processing. Such instructions must not significantly extend the scope of the contract. In the event of any significant extension, the parties will agree on appropriate remuneration for the scopes amended by the supplementary instructions. In such a case, the Contractor must only observe the supplementary instructions after an agreement has been reached.

(3) The Contractor will inform the Customer immediately if, in the Contractor's opinion, an instruction issued by the Customer violates statutory regulations. The Contractor is entitled to refrain from carrying out such an instruction from the Customer until the Customer has sufficiently explained to the Contractor, in writing, how and why the instruction given does not violate any statutory regulation and has again instructed the Contractor, in writing, to implement said instruction. However, the Contractor is not obligated to check the instructions given by the Customer.

(4) Insofar as a claim is made against the Contractor, or against one of their subcontractors, by a third party on the basis of the implementation of an instruction given by the Customer, alleging that said third party has suffered material or immaterial damage due to a violation of the GDPR, or if a supervisory authority imposes or threatens to impose a fine on the Contractor or their subcontractors as a result, the Customer fully indemnifies the Contractor against any such claim or fine. The right to indemnification also includes reasonable costs associated with legal defence. The same applies if a claim is due to a violation of contractual or statutory obligations by the Customer.

6. Sub-contractual relationships

(1) The commissioning of sub-contractors by the Contractor in relation to the processing of Customer Data is only permitted with prior written consent. The Customer has agreed to the commissioning of the subcontractors listed in **Annex 1**.

(2) The Contractor is to carefully select the subcontractor and check prior to commissioning that the subcontractor is able to comply with the agreements made between the Customer and the Contractor.

(3) The Contractor is to obligate the subcontractor, in writing, in the subcontract processing agreement to the same extent as the Contractor is obligated vis-à-vis the Customer under this contract. The subcontract processing agreement directly grants the Customer all monitoring rights in relation to the subcontractor in accordance with section 7 of this contract (genuine contract in favour of third parties). The spheres of responsibility for the Contractor and the subcontractor are to be clearly demarcated in the subcontract processing agreement. Insofar as several subcontractors are used, this also applies to the responsibilities between the individual subcontractors.

(4) The Contractor will conclude contracts with subcontractors, giving due consideration to GDPR Article 44(ff) and specifically on the basis of EU standard contracts, if and insofar as the data collection and/or use by the subcontractor takes place outside the EU or EEA. In such cases, the Customer hereby authorises the Contractor to conclude the standard EU controller to processor contract with the respective subcontractor on behalf of the Customer in such a way that either (i) the Customer becomes party to an existing EU standard contract between the subcontractor (as processor) and the Contractor (as controller) and, in this respect, acquires the same rights as the Contractor under the EU standard contract or (ii) the Customer concludes an EU standard contract directly with the subcontractor and the Contractor enters into it such that the Contractor acquires the same rights as the Customer under the EU standard contract.

(5) Data may only be transferred to the subcontractor if all subcontracting prerequisites have been met and the subcontractor has fulfilled the obligation under section 8 of this contract.

(6) The Contractor has derived monitoring obligations vis-à-vis subcontractors. To this end, the Contractor can and must exercise the monitoring powers of the Customer described in this contract as well as those reflected in the subcontract processing agreement. The Contractor must regularly check the subcontractor's compliance with contractual obligations in a suitable form, document the result of the check, and make the associated report of the check available to the Customer on request. The Customer remains entitled to monitor the exercise of monitoring powers by the Contractor without restriction and may, at any time, also exercise such monitoring themselves vis-à-vis the subcontractor.

(7) The subcontractor's obligation must be set out in writing and be in accordance with GDPR Article 28(2-4). A copy of the written obligation is to be sent to the Customer on request.

(8) Subcontracting relationships within the meaning of this regulation do not include those services which the Contractor utilises with third parties as ancillary services to support performance of the order. Such services include telecommunications services, maintenance and user service, cleaning staff and inspectors, for example. However, to ensure the protection and security of Customer Data, the Contractor is obligated to make appropriate and legally compliant contractual agreements and to take monitoring measures to ensure the protection and security of Customer Data. This obligation also applies to ancillary services which third parties are commissioned to undertake.

(9) The Contractor's notification obligations as per section 4 apply accordingly to data security incidents which occur among their subcontractors.

7. Monitoring powers

(1) The Customer has the right to monitor the processing of Customer Data by the Contractor, including compliance with (i) the statutory provisions relating to data protection, (ii) the contractual provisions agreed between the parties and (iii) the instructions of the Customer, to the extent necessary, or to have the processing monitored by a third party who is obligated to maintain secrecy. The Contractor specifically ensures that the Customer is able to assure themself that the Contractor will comply with their obligations under GDPR Article 28.

(2) The Contractor is obligated to provide information to the Customer on request, insofar as such information is necessary to carry out the check set out in section 1. The fulfilment of this obligation, and specifically proof of implementation of technical and organisational measures, which do not only relate to the specific order, can be effected by

- ☐ compliance with the approved rules of conduct as per GDPR Article 40;
- ☐ certification in accordance with an approved certification procedure as per GDPR Article 42;
- ☐ up-to-date certificates, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officer, IT security department, data protection auditors, quality auditors);
- ☐ suitable certification by IT security or data protection audit (e.g. according to BSI basic protection).

(3) Insofar as there is a justified interest, the Customer may also insist on an inspection of Customer Data processed by the Contractor for the Customer as well as an inspection of the data processing systems and programs used.

(4) In the event of a further interest in inspection beyond the aforementioned substantiation and inspections, the Customer may, subject to prior notification and a reasonable period of notice, have the inspection defined in section 1 carried out at the Contractor's premises during normal business hours by a third party who is obligated to maintain secrecy. Insofar as subcontracting relationships exist, the Contractor will carry out such inspections of the respective business premises on behalf of, and in accordance with, instructions from the Customer. In this regard, the Customer will ensure that the inspections are only carried out to the extent necessary.

(5) Insofar as the Customer and the Contractor are subject to public controls by the competent supervisory authority, the parties will support each other to the best of their ability, on request, within the scope of official supervisory procedures, if and to the extent that the contractual processing of Customer Data is the subject of the supervisory procedure. In this context, the Contractor is also entitled to disclose information relating to instructions given by the Customer.

(6) The Contractor can assert a claim for remuneration for enabling the Customer to carry out inspections.

8. Confidentiality

(1) The Contractor is obligated to maintain confidentiality when processing Customer Data for the Customer. The Customer is obligated to notify the Contractor of any special confidentiality rules.

(2) The Contractor warrants that they are aware of the applicable data protection regulations and are familiar with the application thereof. Furthermore, the Contractor warrants that they will maintain confidentiality as per GDPR Article 28(3)(2)(b), 29, 32(4) and will only employ employees or freelancers in the performance of work if such employees/freelancers have been obligated to maintain confidentiality and have been made familiar with the data protection provisions relevant to them before performing any work.

9. Protection of the rights of data subjects

(1) The Customer is solely responsible for safeguarding the rights of data subjects. Insofar as a data subject contacts the Contractor directly for the purpose of information, correction, erasure or blocking of Customer Data concerning them, the Contractor will forward said request to the Customer no later than on the following working day and will not contact the data subject without corresponding documented individual instructions from the Customer. The Contractor may only provide information to data subjects following prior instruction from the Customer.

(2) Insofar as the cooperation of the Contractor is necessary to protect the rights of data subjects – specifically with regard to information, correction, blocking, erasure or data portability (GDPR Article 15(ff)) – by the Customer, the Contractor will take the requisite measures as instructed by the Customer.

(3) Regulations pertaining to possible remuneration of additional expenses incurred by the Contractor as a result of supplementary instructions from the Customer remain unaffected.

10. Confidentiality obligations

(1) Both parties are obligated to treat all information they receive in connection with performance of this contract as confidential for an unlimited period of time and to use such information solely for performance of the contract. Neither party is entitled to use this information, in whole or in part, for purposes other than those stated or to make this information available to third parties.

(2) The aforementioned obligation does not apply to information which one of the parties has demonstrably obtained from third parties without being obligated to maintain secrecy or to information which is public knowledge.

11. Technical and organisational measures pertaining to data security

(1) The Contractor is obligated to ensure security vis-à-vis the customer as per GDPR Article 28(3)(2)(c), 32 particularly in conjunction with GDPR Article 5(1)(2). On the whole, the measures to be taken are data security measures and measures to ensure a level of protection with regard to confidentiality, integrity, availability and resilience of systems commensurate with the risk. In this regard, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of GDPR Article 32(1) are to be given due consideration [details can be found in Annex 2 attached]. The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. In this regard, the defined measures must not fall short of the safety level. Significant changes are to be documented.

(2) The Contractor documents compliance with the requisite technical and organisational measures defined in Annex 2 prior to commencement with regard to specific performance of the order and transfers said documentation to the Customer if requested to do so. If the Customer accepts the measures as per Annex 2, such measures become the basis of the order.

12. Order term

(1) The contract begins when it comes into force and ends upon termination of the main contract and upon prescription of the post-contractual obligations within the scope of liability for defects.

(2) The Customer can terminate the contract at any time and without notice if there is a serious violation of the applicable data protection regulations or obligations under this contract by the Contractor, if the Contractor is unable or unwilling to carry out an instruction given by the Customer or if the Contractor refuses, in breach of contract, to grant access to the Customer or to the competent supervisory authority.

(3) The Contractor can also terminate the contract at any time and without notice, specifically in the event of a serious violation of the applicable data protection regulations or obligations under this contract by the Customer or if the Customer issues an unlawful instruction and does not depart from said instruction, even after notification has been given by the Contractor.

13. Termination, return and erasure of data provided

(1) The Contractor is prohibited from actively processing Customer Data following termination of this contract; only further storage of Customer Data continues to be permitted until the Contractor has transferred said Customer Data to the Customer as intended or has deleted or destroyed said Customer Data; in such cases the provisions

of this contract continue to apply following termination of the contract until the Contractor no longer has any Customer Data at their disposal.

(2) The Contractor is to completely and irretrievably surrender Customer Data to the Customer or delete or destroy all Customer Data they receive from the Customer as well as all Customer Data acquired in the course of performing the contract and all products of processing and use thereof as soon as such knowledge is no longer necessary for fulfilment of the purpose of the respective data collection and use. However, this is to be done no later than upon completion of the contractual service provision. The parties are aware that it is not always technically possible to delete specific Customer Data (e.g. because said data is contained in back-ups or archives). In such cases, the Contractor is obligated to deactivate the data – insofar as deactivation is possible – or no longer actively use said data or keep said data in a usable state.

(3) The provisions of section 13.2 also apply to copies of Customer Data (specifically archiving and backup files) in all systems of the Contractor as well as to test and reject data with the aforementioned restrictions of a technical nature.

(4) The Contractor documents the measures in accordance with sections 13.2 and 13.3 in a suitable manner and provides the Customer with confirmation that the data carriers and data have been returned or destroyed/deleted completely and in accordance with the contract. The Customer is entitled to check this. Section 7 applies accordingly.

14. Liability

The Customer and the Contractor are liable vis-à-vis data subjects in accordance with the provisions of GDPR Article 82, specifically in accordance with section (2)(2), section (3) and section (5). GDPR Article 28(4)(2) also applies to the internal relationship.

The Contractor is thus responsible, but only and in each case only on the basis of the content agreed in this contract, for the following:

- The processing of data in accordance with instructions and the obligation to inform in the event of unlawful instructions,
- The confidentiality obligation for any authorised persons involved,
- The technical and organisational security measures taken,
- The proper commissioning of subcontractors,
- Assisting in the exercise of data subjects' rights – insofar as agreed in this contract,
- The agreed support, e.g. in relation to reporting data protection incidents,
- Creation and management of a processing directory within the scope of data processing,
- The appointment of their own data protection officer,
- Proper and contract-compliant erasure and/or return of data upon completion of processing and,
- Agreement to and participation in inspections and audits of the data controller.

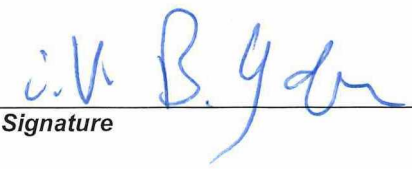
Insofar as the Contractor determines that the purposes and means of processing are in violation of data protection regulations and, in particular, that processing exceeds the instructions of the Customer, the Contractor is deemed to be the data controller with regard to such processing.

15. Final Provisions

1) Changes, additions, and the cancellation of this contract must be made in writing. The same applies to any change to, or cancellation of, the written form requirement.

2) In the event that individual provisions of this contract are or become ineffective, or contain a loophole, this does not affect the remaining provisions. The parties are obligated to replace the invalid provision with a legally permissible provision that comes closest to the purpose of the invalid provision and best meets the requirement of GDPR Article 28.

3) In the event of contradictions between this contract and other agreements between the parties, the provisions of this contract prevail.

Signed for and on behalf of	Signed for an on behalf of
	SCHENCK RoTec GmbH
Company	
Date	*Date*
	
Signature	***Signature***
Name	i. V. Dr. Andy Rüdel *Name*
Title	*Director Business Unit Service* *Title*
	
Signature	***Signature***
Name	i. V. Bernhard Wydra *Name*
Title	*Senior Manager Integrated Management System /* Company Officer for Information Security and Data Protection *Title*

Hereafter:

Annexes 1 and 2 to the contract

Annex 1 to the data processing contract

Regarding section 6 of the contract:

Subcontractor of the Contractor in relation to remote access and/or remote maintenance:

1. DÜRR IT Service GmbH (Bietigheim-Bissingen) as the central IT provider for all companies of the DÜRR Group (Bietigheim-Bissingen) using the following IT system service providers:
   - Arvato Systems GmbH (Gütersloh),
   - T-Systems International GmbH (Frankfurt a.M.),
   - Getronics Germany GmbH (Neu-Isenburg) and
   - Ade Automation (Heilbronn).

2. Depending on the operating site of the machine, system and/or software product, employees of international DÜRR/SCHENCK subsidiaries may also be subject to the same data protection standards and obligations as employees of the company headquarters in Germany.

Annex 2 to the data processing contract

Regarding section 11 of the contract:

Technical and organisational measures to protect personal data

1. Confidentiality (GDPR Article 32(1)(b))

Physical access control

Buildings are secured by means of physical access control involving access cards and access control systems. Visitors are only able to enter the building via the visitor reception area. Buildings are secured externally by means of video camera systems. There are various security zones (open areas: such as meeting rooms, canteen etc.; work areas, such as offices and specially secured areas, such as EDP department, test centre, especially sensitive departments) in the buildings. These zones are separated from each other by locking systems.

A clean desk policy has been implemented which stipulates that documents are not to be left lying unattended in the absence of employees, but rather such documents are to be stored safely. Notebooks and PCs are to be secured or locked with a "Kensington Lock" in the absence of employees.

System access control

A system-supported workflow involving data controllers aids the process of employees joining, transferring to, and leaving the company in conjunction with the granting of access to the relevant data processing units. In particular, this workflow controls basic system authorisations such as user account and Active Directory entries. Complex passwords consisting of at least 10 characters are mandatory for technical reasons. With regard to transfers, existing authorisations are always deleted and new authorisations are granted. Regular checks are envisaged for especially critical authorisations. Authorisation requests are documented either in the ticket system (scanned paper requests) or in the electronic workflow.

There are separate application procedures for local admin rights. A separate, comprehensible justification must be provided by the responsible supervisor upon application.

Data access control

A formalised and standardised authorisation assignment process has been implemented. Application/approval/implementation takes place on the basis of the four eyes principle as a minimum requirement and is documented. The application for, approval, and implementation of authorisations is formally documented. A rights and role concept has been implemented for sensitive systems. This concept minimises conflicts of functional separation. Compliance is checked on a regular basis.

Separation requirement

There is a fundamental separation of development, test and production systems. Furthermore, different systems, system instances and clients exist for relevant systems (SAP, AD, CRM etc.).

Pseudonymisation

Pseudonymisation is carried out as necessary.

4

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

Transfer control

Data transfer within the DÜRR Group is carried out via a secure MPLS or IP-VPN network. Physical data transport (tapes etc.) is not envisaged. Internal rules stipulate that business data is to be stored on designated drives and not on mobile devices.

Hard drives of notebooks and other mobile devices are encrypted.

Data carriers are completely and securely deleted and repeatedly overwritten prior to being transferred or destroyed by the IT departments.

Entry control

A login is implemented for essential systems and applications. However, logs are not evaluated unless there is concrete suspicion. For essential systems and applications, appropriate recording is implemented to ensure traceability, insofar as such recording is technically possible.

All employees are obligated under the terms of their contracts of employment vis-à-vis compliance with data protection regulations. Moreover, Group-wide organisational instructions pertaining to "handling information", "data protection" and "IT security" have been implemented.

Every employee in the Group has completed mandatory web-based training (including a final test) in information security and data protection.

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

Availability control

Needs-based backup/disaster and recovery processes have been implemented for IT systems. Data centres comply with minimum standards, which are prescribed on a Group-wide basis. Such data centres are checked for compliance with the aforementioned standards via internal and external audits. Server and client systems are equipped with up-to-date anti-malware systems. The currency of the systems is continuously monitored and appropriate automated and manual measures are taken in the event of any deviations.

Rapid recoverability

Recovery tests are performed in order to test data recoverability.

4. Procedure for regular checking, analysis and evaluation (GDPR Article 32(1)(d); GDPR Article 25(1))

Order control

Processors are carefully selected by IT/specialist departments and purchasing. An agreement on data processing is concluded with each processor. Such an agreement regulates statutory requirements. Processors must have a comparable safety level to that which is implemented in the DÜRR Group as a minimum requirement.