Vertrag über Auftragsverarbeitung

zwischen der

_____

_____

_____

- Auftraggeberin -

und der

Schenck RoTec GmbH
Landwehrstraße 55
64293 Darmstadt
Deutschland

- Auftragnehmerin -

Die Auftraggeberin betreibt eine Maschine, Anlage und / oder ein Software-Produkt, das von der Auftragnehmerin geliefert wurde. Zwecks Durchführung von Inbetriebnahme- und Service-Tätigkeiten an Maschinen, Anlagen und / oder Software-Produkten der Auftraggeberin wird die Auftragnehmerin bei entsprechendem Anlass zur effizienten Leistungserfüllung auch Online-Fernzugriffe bzw. Fernwartung über eine geschützte Internet-Verbindung einsetzen.

Bei der Fernzugriffsverbindung mit Maschine, Anlage und / oder Software-Produkt der Auftraggeberin kann nicht vollständig ausgeschlossen werden, dass Mitarbeiter der Auftragnehmerin auch personenbezogene Daten zur Kenntnis nehmen, die auf der Maschine, Anlage und / oder im Software-Produkt durch Mitarbeiter des Auftraggebers gespeichert wurden.

Die Parteien vereinbaren daher einen Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO.

Unabhängig von dieser datenschutzrechtlichen Vereinbarung bedarf jeder Geschäftsvorgang mit Online-Fernzugriff auf Maschinen, Anlagen und / oder Software-Produkte einer expliziten Freigabe durch die Auftraggeberin.

1. Allgemeines

(1) Die Auftragnehmerin verarbeitet personenbezogene Daten, für die die Auftraggeberin als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert („**Auftraggeber-Daten**"), im Auftrag und nach Weisung für die Auftraggeberin.

Sofern in diesem Vertrag von „**Datenverarbeitung**", „**verarbeiten**" oder „**Verarbeitung**" (von Auftraggeber-Daten) gesprochen wird, bezieht sich das allgemein auf die Verwendung von personenbezogenen Daten. Eine „**Verwendung**" von Auftraggeber-Daten umfasst insbesondere Erhebung, Speicherung, Übermittlung, Sperrung, Löschung, Anonymisierung, Pseudonymisierung, Verschlüsselung oder sonstige Nutzung von Auftraggeber-Daten.

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/ -kategorien:

Von Mitarbeitern des Auftraggebers ggf. auf Maschine, Anlage und / oder in Software-Produkten gespeicherte Daten, die auch personenbezogene Informationen enthalten können.

2. Gegenstand des Auftrags, Ort der Datenverarbeitung

(1) Der Auftrag der Auftraggeberin an die Auftragnehmerin umfasst die im Hauptvertrag näher beschriebenen Leistungen und/oder die Verpflichtungen im Rahmen der Mängelhaftung aus dem Hauptvertrag. Der Kreis der von der Datenverarbeitung Betroffenen umfasst je nach Art und Inhalt der ggf. auf Maschine, Anlage und / oder in Software-Produkten gespeicherten Daten:

- Mitarbeiter der Auftraggeberin
- Kunden der Auftraggeberin
- Lieferanten der Auftraggeberin

(2) Die Verarbeitung der Auftraggeber-Daten durch die Auftragnehmerin findet ausschließlich in Mitgliedstaaten der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Eine Datenverwendung außerhalb des genannten Gebiets, auch im Wege der Gewährung des Zugriffs auf Auftraggeber-Daten an Personen außerhalb des genannten Gebiets, bedarf der vorherigen schriftlichen Zustimmung der Auftraggeberin. Datenverwendungen in Ländern, die weder Mitgliedstaat der Europäischen Union noch Vertragsstaat des EWR sind („**Drittstaaten**") dürfen nur unter der weiteren Voraussetzung erfolgen, dass die Voraussetzungen der Art. 44 ff. DS-GVO zur Zufriedenheit der Auftraggeberin erfüllt sind.

(3) Die Auftragnehmerin erwirbt an den Auftraggeber-Daten keine Rechte.

3. Rechte und Pflichten der Auftraggeberin

(1) Die Auftraggeberin ist Verantwortlicher (Art. 4 Nr. 7 DS-GVO) für die Verarbeitung von Auftraggeber-Daten im Auftrag durch die Auftragnehmerin.

(2) Die Auftraggeberin steht nach außen, also gegenüber Dritten und den Betroffenen, für die Wahrung der Betroffenenrechte nach Artt. 15 ff. DS-GVO ein. Betroffenenrechte sind daher gegenüber der Auftraggeberin geltend zu machen.

(3) Die Auftraggeberin ist Eigentümerin der Auftraggeber-Daten und im Verhältnis der Parteien zueinander Inhaber aller etwaigen Rechte an den Auftraggeber-Daten.

(4) Für den Fall, dass eine Informationspflicht gegenüber Dritten zum Beispiel nach Art. 34 DS-GVO besteht, ist die Auftraggeberin für die Erfüllung der Pflichten verantwortlich.

4. Pflichten der Auftragnehmerin, Datensicherheit

(1) Die Auftragnehmerin verarbeitet Auftraggeber-Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und entsprechend den Weisungen der Auftraggeberin. Sie hält dabei die gesetzlichen Pflichten, die ihr durch die DS-GVO auferlegt werden, ein. Eine hiervon abweichende Verarbeitung ist der Auftragnehmerin untersagt, es sei denn, dass die Auftraggeberin dieser Verarbeitung in Schriftform zugestimmt hat.

(2) Die Auftragnehmerin darf ohne vorherige schriftliche Zustimmung durch die Auftraggeberin keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen, soweit und solange sie nicht zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Die Auftragnehmerin darf Auftraggeber-Daten ohne vorherige schriftliche Zustimmung durch die Auftraggeberin auch nicht an Dritte oder andere Empfänger aushändigen. Hiervon ausgenommen sind Datenweitergaben an Unterauftragnehmer, deren Beauftragung die Auftraggeberin gemäß Ziffer 6.1 zugestimmt hat.

(3) Die Auftragnehmerin wird die Daten, die sie im Auftrag für die Auftraggeberin verarbeitet, auf geeignete Weise kennzeichnen und von sonstigen Datenbeständen getrennt halten.

(4) Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird die Auftragnehmerin die Daten mit dem jeweiligen Zweck kennzeichnen

(5) Die Auftragnehmerin hat der Auftraggeberin auf Verlangen ein jeweils aktuelles Verzeichnis nach Art. 30 Abs. 2 und 3 DS-GVO zur Verfügung zu stellen.

(6) Die Auftragnehmerin bestätigt, dass sie einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 DS-GVO bestellt hat, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Diesen erreichen Sie unter SCHENCK RoTec GmbH, Landwehrstraße 55, 64293 Darmstadt, Tel.-Nr. +49 6151 32-0, Datenschutzbeauftragter oder unter dataprotection@schenck.net. Die Auftragnehmerin verpflichtet sich, die Bestellung eines betrieblichen Datenschutzbeauftragten während der Dauer des Vertrages aufrecht zu erhalten. Einen Wechsel in der Person des betrieblichen Datenschutzbeauftragten hat die Auftraggeberin der Auftragnehmerin in Textform mitzuteilen.

(7) Die Auftragnehmerin ist verpflichtet, ihr Unternehmen und ihre Betriebsabläufe so zu gestalten, dass die Auftraggeber-Daten im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Die Auftragnehmerin wird die Auftraggeberin über Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, rechtzeitig vorab informieren.

(8) Die Auftragnehmerin ist verpflichtet, der Auftraggeberin jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen der Auftraggeberin mitzuteilen, der im Zuge der Verarbeitung von Daten durch sie oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(9) Für den Fall, dass die Auftragnehmerin feststellt oder zu der Annahme kommt, dass von ihr für die Auftraggeberin verarbeitete

- besondere Arten personenbezogener Daten (Art. 9 DS-GVO) oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten (Art. 10 DS-GVO) beziehen

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind oder Datenverarbeitungsvorgänge erfolgen, die einer Datenschutzfolgenabschätzung bedürfen, hat die Auftragnehmerin die Auftraggeberin spätestens am folgenden Werktag über Zeitpunkt, Art und Umfang in Schrift- oder Textform (Fax/E-Mail) zu informieren. Die Auftragnehmerin ist überdies verpflichtet, dabei auch mitzuteilen, welche Maßnahmen durch die Auftragnehmerin getroffen wurden, um dies künftig zu verhindern, sofern dies in Ihrem Aufgabenbereich ist und nicht einer Weisung durch die Auftraggeberin gemäß Ziffer 5 Abs. 1 bedarf.

(10) Die Auftragnehmerin ist verpflichtet, der Auftraggeberin eine Verletzung des Schutzes personenbezogener Daten spätestens am folgenden Werktag zu melden und sie bei ihren diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen auf erstes Anfordern im Rahmen des Zumutbaren und der vertraglichen Vereinbarungen zwischen den Parteien zu unterstützen. Die Auftragnehmerin wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der Auftraggeber-Daten zu minimieren und zu beseitigen, die Auftraggeber-Daten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen.

5. Umfang der Weisungsbefugnis

(1) Mündliche Weisungen bestätigt die Auftraggeberin unverzüglich (mind. Textform). Die Auftragnehmerin darf davon ausgehen, dass Personen, die ihr gegenüber Weisungen erteilen auch hierzu berechtigt sind.

(2) Die Auftraggeberin hat das Recht, ergänzende Weisungen über Art und Umfang der Datenverarbeitung zu erteilen. Diese dürfen den Umfang des Vertrages nicht mehr als unwesentlich erweitern. Im Falle einer wesentlichen Erweiterung einigen sich die Parteien auf eine angemessene Vergütung für die durch die ergänzenden Weisungen geänderten Umfänge. Die Auftragnehmerin muss die ergänzenden Weisungen in diesem Fall erst nach erfolgter Einigung beachten.

(3) Die Auftragnehmerin wird die Auftraggeberin unverzüglich darüber informieren, wenn eine von der Auftraggeberin erteilte Weisung nach ihrer Auffassung gegen gesetzliche Regelungen verstößt. Die Auftragnehmerin ist berechtigt, eine solche Weisung der Auftraggeberin so lange nicht auszuführen, bis die Auftraggeberin ihr hinreichend schriftlich dargelegt hat, dass und warum die erteilte Weisung nicht gegen eine gesetzliche Regelung verstößt und sie erneut und schriftlich angewiesen hat, diese Weisung umzusetzen. Es besteht jedoch keine Prüfpflicht der Auftragnehmerin in Bezug auf die erteilten Weisungen der Auftraggeberin.

(4) Sollte die Auftragnehmerin oder eine ihrer Unterauftragnehmer auf Grund der Umsetzung einer Weisung der Auftraggeberin von einem Dritten mit der Behauptung in Anspruch genommen werden, dass ihm wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, oder eine Aufsichtsbehörde infolgedessen eine Geldbuße gegen die Auftragnehmerin oder deren Unterauftragnehmer verhängen oder androhen, stellt die Auftraggeberin den in Anspruch Genommenen vollumfänglich von einer solchen Inanspruchnahme bzw. der Geldbuße frei. Der Freistellungsanspruch umfasst dabei auch die angemessenen Kosten der Rechtsverteidigung. Entsprechendes gilt, wenn eine Inanspruchnahme auf eine Verletzung der vertraglichen oder gesetzlichen Pflichten durch die Auftraggeberin zurückzuführen ist.

6. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern hinsichtlich der Verarbeitung von Auftraggeber-Daten durch die Auftragnehmerin ist nur mit vorheriger schriftlicher Zustimmung zulässig. Der Beauftragung der in **Anlage 1** genannten Unterauftragnehmer hat die Auftraggeberin zugestimmt.

(2) Die Auftragnehmerin hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeberin und Auftragnehmerin getroffenen Vereinbarungen einhalten kann.

(3) Die Auftragnehmerin hat den Unterauftragnehmer in dem Unterauftragsverarbeitungsvertrag schriftlich ebenso zu verpflichten, wie auch die Auftragnehmerin aufgrund dieses Vertrags gegenüber der Auftraggeberin verpflichtet ist. Der Auftraggeberin sind im Unterauftragsverarbeitungsvertrag gegenüber dem Unterauftragnehmer unmittelbar sämtliche Kontrollrechte gemäß Ziffer 7 dieses Vertrags einzuräumen (echter Vertrag zugunsten Dritter). In dem Unterauftragsverarbeitungsvertrag sind die Verantwortlichkeitssphären der Auftragnehmerin und des Unterauftragnehmers klar voneinander abzugrenzen. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen den einzelnen Unterauftragnehmern.

(4) Die Auftragnehmerin wird ggf. Verträge mit Unterauftragnehmern unter Berücksichtigung der Art. 44 DS-GVO ff. insbesondere auf Basis von EU-Standardverträgen abschließen, wenn und soweit die Datenerhebung und/oder Verwendung durch den Unterauftragnehmer außerhalb der EU bzw. des EWR erfolgt. Für diesen Fall ermächtigt die Auftraggeberin die Auftragnehmerin hiermit, den EU-Standardvertrag

Controller to Processor in Stellvertretung für die Auftraggeberin mit dem jeweiligen Unterauftragnehmer in der Form abzuschließen, dass entweder (i) die Auftraggeberin einem zwischen dem Unterauftragnehmer (als Processor) und der Auftragnehmerin (als Controller) bestehenden EU-Standardvertrag beitritt und insoweit dieselben Rechte wie die Auftragnehmerin unter dem EU-Standardvertrag erwirbt, oder (ii) die Auftraggeberin direkt mit dem Unterauftragnehmer einen EU-Standardvertrag abschließt und die Auftragnehmerin diesem betritt, so dass diese insoweit dieselben Rechte wie die Auftraggeberin unter dem EU-Standardvertrag erwirbt.

(5) Eine Übergabe von Daten an den Unterauftragnehmer ist erst zulässig, wenn alle Voraussetzungen für eine Unterbeauftragung vorliegen und der Unterauftragnehmer die Verpflichtung nach Ziffer 8 dieses Vertrags erfüllt hat.

(6) Die Auftragnehmerin hat abgeleitete Kontrollpflichten gegenüber den Unterauftragnehmern und kann und muss hierfür die in diesem Vertrag beschriebenen, und in dem Unterauftragsverarbeitungsvertrag zu spiegelnden Kontrollbefugnisse der Auftraggeberin wahrnehmen. Die Auftragnehmerin hat die Einhaltung der vertraglichen Verpflichtungen des Unterauftragnehmers regelmäßig in geeigneter Form zu überprüfen, das Ergebnis der Prüfung zu dokumentieren und den entsprechenden Prüfbericht der Auftraggeberin auf Anfrage zur Verfügung zu stellen. Die Auftraggeberin bleibt berechtigt, die Ausübung der Kontrollbefugnisse durch die Auftragnehmerin uneingeschränkt zu überwachen und kann jederzeit auch selbst diese Kontrolle gegenüber der Unterauftragnehmerin ausüben.

(7) Die Verpflichtung des Unterauftragnehmers muss schriftlich und nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO erfolgen. Der Auftraggeberin ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

(8) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistung, Wartung und Benutzerservice, Reinigungskräfte oder Prüfer. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(9) Die Mitteilungspflichten der Auftragnehmerin gemäß Ziffer 4 gelten entsprechend für Datensicherheitsvorfälle, die sich bei ihren Unterauftragnehmern ereignen.

7. Kontrollbefugnisse

(1) Die Auftraggeberin hat das Recht, die Verarbeitung von Auftraggeber-Daten durch die Auftragnehmerin einschließlich der Einhaltung (i) der gesetzlichen Vorschriften zum Datenschutz, (ii) der zwischen den Parteien getroffenen vertraglichen Regelungen und (iii) der Weisungen der Auftraggeberin durch die Auftragnehmerin im erforderlichen Umfang zu kontrollieren oder durch einen zur Verschwiegenheit verpflichteten Dritten kontrollieren zu lassen. Die Auftragnehmerin stellt insbesondere sicher, dass sich die Auftraggeberin von der Einhaltung der Pflichten der Auftragnehmerin nach Art. 28 DS-GVO überzeugen kann.

(2) Die Auftragnehmerin ist der Auftraggeberin gegenüber auf Anforderung zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist. Die Erfüllung dieser Verpflichtung, insbesondere auch der Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(3) Die Auftraggeberin kann bei begründetem Interesse darüber hinaus eine Einsichtnahme in die von der Auftragnehmerin für die Auftraggeberin verarbeiteten Auftraggeber-Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Die Auftraggeberin kann bei einem über die vorstehenden Nachweise und Einsichtnahmen hinausgehenden weiteren Kontrollinteresse nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte der Auftragnehmerin zu den jeweils üblichen Geschäftszeiten von einem zur Verschwiegenheit verpflichteten Dritten vornehmen lassen. Wenn Unterauftragsverhältnisse bestehen, dann wird die Auftragnehmerin im Auftrag und nach Weisungen der Auftraggeberin diese Kontrollen der jeweiligen Betriebsstätte(n) durchführen. Die Auftraggeberin wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden.

(5) Soweit die Auftraggeberin und die Auftragnehmerin öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde unterliegen, werden sie sich auf jeweiliges Verlangen gegenseitig im Rahmen von behördlichen Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten Gegenstand des Aufsichtsverfahrens ist. Die Auftragnehmerin ist dabei berechtigt, auch Informationen zu Weisungen der Auftraggeberin offenzulegen.

(6) Für die Ermöglichung von Kontrollen der Auftraggeberin kann die Auftragnehmerin einen Vergütungsanspruch geltend machen.

8. Vertraulichkeit

(1) Die Auftragnehmerin ist bei der Verarbeitung von Auftraggeber-Daten für die Auftraggeberin zur Wahrung der Vertraulichkeit verpflichtet. Die Auftraggeberin ist verpflichtet, der Auftragnehmerin etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Die Auftragnehmerin sichert zu, dass ihr die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und sie mit der Anwendung dieser vertraut ist. Die Auftragnehmerin sichert ferner zu, dass sie die Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO wahrt und bei der Durchführung der Arbeiten nur Beschäftigte bzw. freie Mitarbeiter einsetzt, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

9. Wahrung von Betroffenenrechten

(1) Die Auftraggeberin ist für die Wahrung der Betroffenenrechte allein verantwortlich. Soweit ein Betroffener sich unmittelbar an die Auftragnehmerin zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Auftraggeber-Daten wenden sollte, wird die Auftragnehmerin dieses Ersuchen spätestens am folgenden Werktag an die Auftraggeberin weiterleiten und ohne entsprechende dokumentierte Einzelweisung der Auftraggeberin nicht mit dem Betroffenen in Kontakt treten. Die Auftragnehmerin darf Auskünfte an Betroffene nur nach vorheriger Weisung durch die Auftraggeberin erteilen.

(2) Soweit eine Mitwirkung der Auftragnehmerin für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung, Löschung oder Datenportabilität (Artt. 15 ff. DS-GVO) – durch die Auftraggeberin erforderlich ist, wird die Auftragnehmerin die jeweils erforderlichen Maßnahmen nach Weisung der Auftraggeberin treffen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen der Auftraggeberin bei der Auftragnehmerin entstehen, bleiben unberührt.

10. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrags erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrags zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

11. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Die Auftragnehmerin verpflichtet sich gegenüber der Auftraggeberin, die Sicherheit gem. Artt. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten ergeben sich aus der beigefügten Anlage 2]. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Auftragnehmerin gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(2) Die Auftragnehmerin dokumentiert die Einhaltung der in Anlage 2 festgelegten, erforderlichen technischen und organisatorischen Maßnahmen vor Beginn hinsichtlich der konkreten Auftragsdurchführung und übergibt diese Dokumentation der Auftraggeberin auf Verlangen. Akzeptiert die Auftraggeberin die Maßnahmen nach Anlage 2, werden sie Grundlage des Auftrags.

12. Dauer des Auftrags

(1) Der Vertrag beginnt mit Inkrafttreten und endet mit Beendigung des Hauptvertrags und Verjährung der nachvertraglichen Verpflichtungen im Rahmen der Mängelhaftung.

(2) Die Auftraggeberin kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der Auftragnehmerin gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, die Auftragnehmerin eine Weisung der Auftraggeberin nicht ausführen kann oder will oder die Auftragnehmerin den Zutritt der Auftraggeberin oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

(3) Ebenso kann die Auftragnehmerin den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, insbesondere wenn ein schwerwiegender Verstoß der Auftraggeberin gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt oder wenn die Auftraggeberin eine gesetzeswidrige Weisung erteilt und von dieser auch nach Hinweis durch die Auftragnehmerin nicht abweicht.

13. Beendigung, Rückgabe und Löschung überlassener Daten

(1) Der Auftragnehmerin ist es untersagt, nach Beendigung dieses Vertrags Auftraggeber-Daten aktiv zu verarbeiten; nur eine weitere Speicherung der Auftraggeber-Daten bleibt zugelassen, bis die Auftragnehmerin diese Auftraggeber-Daten bestimmungsgemäß an die Auftraggeberin herausgegeben oder sie gelöscht oder vernichtet hat; in diesem Fall gelten die Bestimmungen dieses Vertrags auch nach Beendigung des Vertrags bis zu dem Zeitpunkt weiter, in dem die Auftragnehmerin über keinerlei Auftraggeber-Daten mehr verfügt.

(2) Die Auftragnehmerin hat sämtliche ihr von der Auftraggeberin überlassenen sowie sämtliche im Zuge der Vertragsdurchführung hinzugewonnenen Auftraggeber-Daten und alle Verarbeitungs- und Nutzungsergebnisse hieraus vollständig und unwiederbringlich an die Auftraggeberin herauszugeben bzw. zu löschen bzw. zu vernichten, sobald ihre Kenntnis für die Erfüllung des Zwecks der jeweiligen Erhebung und Verwendung nicht mehr erforderlich ist, spätestens jedoch nach Beendigung der vertragsgegenständlichen Leistungserbringung. Den Parteien ist bekannt, dass es technisch nicht immer möglich ist, gezielt Daten der Auftraggeberin zu löschen (z.B. weil diese Daten in Back-ups oder Archiven enthalten sind). In diesen Fällen verpflichtet sich die Auftragnehmerin, die Daten – soweit möglich – zu deaktivieren bzw. nicht mehr aktiv zu nutzen oder nutzbar zu erhalten.

(3) Die Bestimmungen der Ziffer 13.2 gelten auch für Vervielfältigungen der Auftraggeber-Daten (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen der Auftragnehmerin sowie für Test- und Ausschussdaten mit den oben genannten Einschränkungen technischer Art.

(4) Die Auftragnehmerin dokumentiert die Maßnahmen nach Ziffer 13.2 und 13.3 in geeigneter Weise und bestätigt der Auftraggeberin die vollständige und vertragsgemäße Rückgabe bzw. Vernichtung/Löschung der Datenträger und Daten. Die Auftraggeberin ist befugt, dies zu kontrollieren. Ziffer 7 gilt entsprechend.

14. Haftung

Auftraggeberin und Auftragnehmerin haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung, insbesondere gemäß Abs. 2 S. 2, Abs. 3 und Abs. 5. Im Innenverhältnis gilt zudem Art. 28 Abs. 4 S. 2 DS-GVO.

Die Auftragnehmerin verantwortet daher insbesondere, aber auch nur und jeweils nur auf Grundlage der in diesem Vertrag vereinbarten Inhalte:

- Die weisungsmäßige Verarbeitung der Daten und ihre Hinweispflicht bei rechtswidrigen Weisungen,
- Die Vertraulichkeitsverpflichtung der beteiligten befugten Personen,
- Die ergriffenen technischen und organisatorischen Schutzmaßnahmen,
- Die ordnungsgemäße Beauftragung von Unterauftragnehmern,
- Die Mithilfe bei Wahrnehmung von Betroffenenrechten – soweit in diesem Vertrag vereinbart,
- Die vereinbarte Unterstützung zum Beispiel bei Meldung von Datenschutzvorfällen,
- Erstellung und Führung eines Verarbeitungsverzeichnisses im Rahmen der Auftragsverarbeitungen,
- Die Bestellung eines eigenen Datenschutzbeauftragten,
- Ordnungs- und vertragsgemäße Löschung und / oder Rückgabe von Daten nach Abschluss der Verarbeitung sowie,
- Duldung und Mitwirkung bei Prüfungen und Audits des für die Verarbeitung Verantwortlichen.

4

Die Auftragnehmerin gilt, wenn sie unter Verstoß gegen datenschutzrechtliche Regelungen die Zwecke und Mittel der Verarbeitung bestimmt und insbesondere die Weisungen der Auftraggeberin überschreitet, in Bezug auf diese Verarbeitung als Verantwortliche.

15. Schlussbestimmungen

1) Änderungen, Ergänzungen und die Aufhebung dieses Vertrags bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DS-GVO am besten gerecht wird.

3) Im Fall von Widersprüchen zwischen diesen Vertrag und sonstigen Vereinbarungen zwischen den Parteien, gehen die Regelungen dieses Vertrags vor.

Unterzeichnet für und im Namen von	Unterzeichnet für und im Namen von
	SCHENCK RoTec GmbH
Firma	*Firma*
Datum	*Datum*
Unterschrift	***Unterschrift***
	i. V. Dr. Andy Rüdel
Name	*Name*
	Director Business Unit Service
Funktion	*Funktion*
Unterschrift	***Unterschrift***
	i. V. Bernhard Wydra
Name	*Name*
	Senior Manager Integriertes Managementsystem/ Betriebsbeauftragter für Informationssicherheit und Datenschutzbeauftragter
Funktion	*Funktion*

Nachfolgend:

Anlagen 1 bis 2 zum Vertrag

Anlage 1 zum Vertrag über Auftragsverarbeitung

Zu Ziffer 6 des Vertrags:

Subunternehmer der Auftragnehmerin bei Fernzugriff bzw. Fernwartung:

1. DÜRR IT Service GmbH (Bietigheim-Bissingen) als zentraler IT-Provider für alle Gesellschaften der DÜRR-Gruppe (Bietigheim-Bissingen) mit Nutzung folgender IT-System-Dienstleister:
   - Arvato Systems GmbH (Gütersloh),
   - T-Systems International GmbH (Frankfurt a.M.),
   - Getronics Germany GmbH (Neu-Isenburg) und
   - Ade Automation (Heilbronn).

2. Je nach Betriebsstandort von Maschine, Anlage und / oder Software-Produkt ggf. auch Mitarbeiter internationaler DÜRR- / SCHENCK-Tochtergesellschaften, die denselben Datenschutz-Standards und Verpflichtungen unterliegen wie die Mitarbeiter der Unternehmenszentralen in Deutschland.

Anlage 2 zum Vertrag über Auftragsverarbeitung

Zu Ziffer 11 des Vertrags:

Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Gebäude sind mit Zutrittssicherung mittels Zugangskarte und Vereinzelungsanlagen gesichert. Besucher kommen ausschließlich über den Besucherempfang ins Gebäude. Gebäude sind außen mit Videokamerasystemen gesichert. In den Gebäuden gibt es verschiedene Sicherheitszonen (offene Bereiche: wie Besprechungsräume, Kantine etc.; Arbeitsbereiche, wie Büroräumlichkeiten und speziell gesicherte Bereiche, wie Rechenzentrum, Testcenter, besonders sensible Abteilungen) welche durch Schließsysteme voneinander getrennt sind.

Es ist eine Clean Desk Policy implementiert, welche festlegt, dass Unterlagen bei Abwesenheit der Mitarbeiter nicht offen liegen gelassen werden, sondern sicher zu verstauen sind. Notebooks, PCs sind bei Abwesenheit mittels „Kensington Lock" zu sichern oder einzuschließen.

Zugangskontrolle

Ein systemgestützter Workflow unter Einbindung der Verantwortlichen unterstützt den Ein-, Versetzungs-, und Austrittsprozess von Mitarbeitern in Verbindung mit der Zuordnung von Zugriffen auf die relevanten Datenverarbeitungsanlagen. Insbesondere werden hierdurch die grundlegenden Systemberechtigungen wie User-Account und Active Directory-Einträge gesteuert. Komplexe Passwörter mit mind. 10 Stellen sind technisch verpflichtend vorgesehen. Bei Versetzungen werden grundsätzlich bestehende Berechtigungen gelöscht und neue Berechtigungen gegeben. Für besonders kritische Berechtigungen sind regelmäßige Überprüfungen vorgesehen. Berechtigungsanträge werden entweder im Ticketsystem (eingescannte Papieranträge) oder im elektronischen Workflow dokumentiert.

Es gibt gesonderte Beantragungsverfahren für lokale Adminrechte. Es muss bei Beantragung eine gesonderte nachvollziehbare Begründung durch den verantwortlichen Vorgesetzten erfolgen.

Zugriffskontrolle

Es ist ein formalisierter und standarisierter Berechtigungsvergabeprozess implementiert. Beantragung / Genehmigung / Umsetzung findet mindestens im 4-Augenprinzip statt und wird dokumentiert. Die Beantragung, Genehmigung und Umsetzung der Berechtigungen wird formell dokumentiert. Für sensible Systeme ist ein Rechte- und Rollenkonzept implementiert, welches Funktionstrennungskonflikte minimiert. Die Einhaltung wird regelmäßig überprüft.

Trennungsgebot

Es wird grundsätzlich zwischen Entwicklungs-, Test- und Produktivsystemen getrennt. Ferner existieren für relevante Systeme (SAP, AD, CRM etc.) verschiedene Systeme, Systeminstanzen oder Mandanten.

Pseudonymisierung

Eine Pseudonymisierung wird vorgenommen, wo es notwendig ist.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Die Datenübertragung innerhalb der DÜRR-Gruppe erfolgt über ein gesichertes MPLS oder IP-VPN Netzwerk. Physische Datentransporte (Bänder etc.) sind nicht vorgesehen. Interne Regeln schreiben vor, dass Geschäftsdaten auf den dafür vorgesehenen Laufwerken und nicht auf mobilen Geräten zu speichern sind.

Festplatten von Notebooks und anderen mobilen Endgeräten sind verschlüsselt.

Datenträger werden vor der Weitergabe oder Vernichtung durch die IT-Stellen vollständig und gesichert gelöscht und mehrfach überschrieben.

Eingabekontrolle

Für wesentliche Systeme und Applikationen ist ein Login implementiert. Logs werden jedoch nicht ohne spezifischen Verdacht ausgewertet. Für wesentliche Systeme und Applikationen sind, wenn technisch möglich, entsprechende Protokollierungen implementiert, um die Nachvollziehbarkeit zu gewährleisten.

Alle Mitarbeiter werden hinsichtlich der Einhaltung von Regelungen zum Datenschutz arbeitsvertraglich verpflichtet. Ferner sind konzernweit gültige Organisationsanweisungen zum Thema „Umgang mit Informationen", „Datenschutz" und „IT-Security" implementiert.

Jeder Mitarbeiter im Konzern hat im ein verpflichtendes web-based Training (inkl. abschließendem Test) zum Thema Informationssicherheit und Datenschutz absolviert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Für IT Systeme sind bedarfsgerechte Backup- / Desaster- und Recovery-Prozesse implementiert. Rechenzentren entsprechen Mindeststandards, welche konzernweit vorgeschrieben sind und werden hinsichtlich Einhaltung dieser Standards durch interne und externe Audits überprüft. Es sind Server- und Clientsysteme mit aktuellen Anti-Malwaresystemen ausgestattet. Die Aktualität der Systeme wird kontinuierlich überwacht und im Falle von Abweichungen werden entsprechende automatisierte und manuelle Maßnahmen ergriffen.

Rasche Wiederherstellbarkeit

Es werden Recovery Tests durchgeführt, um die Wiederherstellbarkeit von Daten zu erproben.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Auftragskontrolle

Auftragsverarbeiter werden sorgfältig durch IT/Fachbereich und Einkauf ausgewählt. Mit jedem Auftragsverarbeiter wird eine Vereinbarung zur Auftragsverarbeitung geschlossen, in welcher die gesetzlichen Vorgaben geregelt sind. Auftragsverarbeiter müssen mindestens ein vergleichbares Sicherheitsniveau aufweisen, wie es in der DÜRR-Gruppe implementiert ist.