rocon software development GmbH
Neumühler Weg 14
66130 Saarbrücken

saarbruecken@rocongruppe.de
www.rocongruppe.de

Vereinbarung zur Auftragsdatenverarbeitung

zwischen der Firma

rocon software development GmbH
Neumühler Weg 14
66130 Saarbrücken

- Nachstehend einzeln **Auftragnehmerin** genannt **-**

und

dem jeweiligen die Cloud Services nutzenden Unternehmen

- nachstehend einzeln **Auftraggeberin** genannt –
- gemeinsam **Parteien** genannt –

1 Gegenstand und Dauer des Auftrags

1.1 Die Auftragnehmerin führt die im Anhang 1 beschriebenen Dienstleistungen für die Auftraggeberin durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

1.2 Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet.

2 Weisungen der Auftraggeberin

2.1 Die Auftraggeberin ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

2.2 Die Auftragnehmerin verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen der Auftraggeberin und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn die Auftraggeberin dies anweist.

2.3 Die Verarbeitung erfolgt nur auf Weisung der Auftraggeberin, es sei denn, die Auftragnehmerin ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

2.4 Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von der Auftraggeberin zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn die Auftragnehmerin dies verlangt.

2.5 Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Vorschriften verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen.

3 Technische und organisatorische Maßnahmen (TOM)

3.1 Die Auftragnehmerin verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und im Anhang 3 dieses Vertrages zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

3.2 Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Auftragnehmerin darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss die Auftragnehmerin der Auftraggeberin nur wesentliche Anpassungen mitteilen.

3.3 Die Auftragnehmerin unterstützt die Auftraggeberin bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Die Auftragnehmerin hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten der Auftraggeberin mitzuwirken. Die Auftragnehmerin wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat der Auftraggeberin alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

4 Pflichten der Auftragnehmerin

4.1 Die Auftragnehmerin bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

4.2 Die Auftragnehmerin bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

4.3 Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

4.4 Die Auftragnehmerin darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten der Auftraggeberin zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

4.5 Soweit gesetzlich vorgeschrieben, bestellt die Auftragnehmerin einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden der Auftraggeberin zum Zweck der direkten Kontaktaufnahme mitgeteilt.

4.6 Die Auftragnehmerin darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

4.7 Die Auftragnehmerin unterstützt die Auftraggeberin mit geeigneten technischen und organisatorischen Maßnahmen, damit diese ihre bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Die Auftragnehmerin benennt einen Ansprechpartner, der die Auftraggeberin bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt der Auftraggeberin dessen Kontaktdaten unverzüglich mit. Soweit die Auftraggeberin besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt die Auftragnehmerin die Auftraggeberin hierbei. Auskünfte an die betroffene Person oder Dritte darf die Auftragnehmerin nur nach vorheriger Weisung der Auftraggeberin erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

5 Berechtigung zur Begründung von Unterauftragsverhältnissen

5.1 Die Auftragnehmerin darf Unterauftragnehmer nur beauftragen, wenn sie die Auftraggeberin immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch die Auftraggeberin die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen. Ein wichtiger Grund ist beispielsweise: Wenn die Auftraggeberin mit dem Unterauftragsnehmer in Konkurrenz steht.

5.2 Ein Unterauftragsverhältnis liegt insbesondere vor, wenn die Auftragnehmerin weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. 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. Telekommunikationsleistungen oder Reinigungskräfte.

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.

5.3 Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn die Auftragnehmerin durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

5.4 Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

6 Kontrollrechte der Auftraggeberin

6.1 Die Auftragnehmerin erklärt sich damit einverstanden, dass die Auftraggeberin oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen der Auftragnehmerin zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung.

6.2 Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann ebenfalls der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung. In besonderen Fällen (Beispiel: Datenpanne) ist die Auftraggeberin berechtigt, eine unangekündigte vor-Ort-Kontrolle vorzunehmen.

7 Mitzuteilende Verstöße der Auftragnehmerin

7.1 Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten der Auftraggeberin mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten der Auftraggeberin.

7.2 Gleiches gilt, wenn die Auftragnehmerin feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Der Auftragnehmerin ist bekannt, dass die Auftraggeberin verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden.

7.3 Sofern es zu solchen Verletzungen gekommen ist, wird die Auftragnehmerin die Auftraggeberin bei der Einhaltung ihrer Meldepflichten unterstützen. Sie wird die Verletzungen der Auftraggeberin unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,
b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

8 Beendigung des Auftrags

8.1 Nach Abschluss der Auftragsverarbeitung hat die Auftragnehmerin alle personenbezogenen Daten nach Wahl der Auftraggeberin entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

8.2 Die Auftraggeberin kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn die Auftragnehmerin einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeberin aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

9 Schlussbestimmungen

9.1 Sollte das Eigentum der Auftraggeberin bei der Auftragnehmerin durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin die Auftraggeberin unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände der Auftraggeberin ausgeschlossen.

9.2 Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was seit dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.

9.3 Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

rocon software development GmbH
Neumühler Weg 14
66130 Saarbrücken

saarbruecken@rocongruppe.de
www.rocongruppe.de

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

1 Gegenstand der Verarbeitung

1.1 Gegenstand und Dauer der Verarbeitung ergibt sich aus den AGB sowie aus den Regelungen des Hauptvertrags.

2 Art und Zweck der Verarbeitung

2.1 Die rocon software development GmbH kann bei folgenden Leistungen mit personenbezogenen Daten, die bei der Auftraggeberin gespeichert sind, in Berührung kommen:

- Unterstützung bei der Durchführung von Verträgen oder Aufträgen
- Vertrieb oder Versand von Waren oder Erbringung von Leistungen
- Betreuung von Kunden und Geschäftspartnern
- Gewährleistung der ordentlichen und gesetzeskonformen Buchhaltung
- Rechnungsstellung für Waren oder Leistungen
- Pflege und Verwaltung von Beschäftigtendaten
- Dokumentation von Arbeitszeiten
- Zahlung von Gehältern und Löhnen
- Planung und Verwaltung von Fortbildungs- und Trainingsmaßnahmen
- Dokumentation und Festlegung von Compensations und Benefits für Beschäftigte
- Überwachung betrieblicher Einrichtungen
- Gewährleistung des Zutrittsschutzes
- Gewährleistung der ordnungsgemäßen Akten- und Datenträgervernichtung
- Kommunikation mittels elektronischer Medien
- Ermöglichung der Kontaktierung von Beschäftigten
- Dokumentation von Terminen von Beschäftigten
- Zugangsverwaltung hinsichtlich Technik (einschließlich Telekommunikation, Netzwerk)

3 Art der Daten

3.1 Die rocon software development GmbH kann mit folgenden Kategorien personenbezogener Daten und Datenarten in Berührung kommen

- Stammdaten (Adressen)
- Personal- und Identifikationsnummern
- Vertragsdaten
- E-Mails

rocon software development GmbH
Neumühler Weg 14
66130 Saarbrücken

saarbruecken@rocongruppe.de
www.rocongruppe.de

4 Kategorien betroffener Personen

4.1 Die rocon software development GmbH kann mit folgenden Kategorien betroffener Personen in Berührung kommen

- Beschäftigte
- Auszubildende und Praktikanten
- freie Mitarbeiter
- Gesellschafter, Organe der Gesellschaft
- Kunden
- Interessenten
- Lieferanten und Dienstleister
- Mieter
- Geschäftspartner
- externe Berater

5 Datenschutzbeauftragter

Dr. Uwe Schläger
datenschutz nord GmbH
Konsul-Smidt-Straße 88
28213 Bremen
Tel. 0421 6966 32 212
Email: USchlaeger@datenschutz-nord.de

rocon software development GmbH
Neumühler Weg 14
66130 Saarbrücken

saarbruecken@rocongruppe.de
www.rocongruppe.de

Anhang 2: Liste der beauftragten Unterauftragnehmer

1 Verbundene Unternehmen

Unterauftragnehmer	Verarbeitungsstandort	Art der Dienstleistung
rocon besitz holding GmbH	27356 Rotenburg (Wümme)	Beratung, Support und Projektarbeit zu Kaufmännischen Lösungen
rocon business solutions GmbH	27356 Rotenburg (Wümme)	Beratung, Support und Projektarbeit zu Kaufmännischen Lösungen
rocon smart business software GmbH	27356 Rotenburg (Wümme)	Beratung, Support und Projektarbeit zu Kaufmännischen Lösungen
rocon service + büro GmbH	06844 Dessau-Roßlau	Beratung, Support und Projektarbeit zu Kaufmännischen Lösungen

2 Newsletterversand

Unterauftragnehmer	Verarbeitungsstandort	Art der Dienstleistung
rapidmail GmbH	79098 Freiburg i.Br.	Kunden-Informations-Emails zu Produkten und Dienstleistungen der rocongruppe

3 Datenträgervernichtung

Unterauftragnehmer	Verarbeitungsstandort	Art der Dienstleistung
documentus GmbH	28197 Bremen	Vernichtung von Datenträgern aller Art

4 Infrastruktur und Plattformdienste

Unterauftragnehmer	Verarbeitungsstandort	Art der Dienstleistung
Amazon Web Services EMEA SARL ("AWS EUROPE")	Siehe Zusatz unter 4.1	Infrastruktur-, Plattform- und Softwareleistungen, IaaS/PaaS/SaaS
Microsoft	Siehe Zusatz unter 4.1	Infrastruktur-, Plattform- und Softwareleistungen, IaaS/PaaS/SaaS
d.velop AG, Gescher	Siehe Zusatz unter 4.1	Infrastruktur-, Plattform- und Softwareleistungen, IaaS/PaaS/SaaS

rocon software development GmbH
Neumühler Weg 14
66130 Saarbrücken

saarbruecken@rocongruppe.de
www.rocongruppe.de

4.1 Für die Infrastruktur- und Plattformleistungen werden von den Unterauftragnehmern ausschließlich Rechenzentren innerhalb der EU genutzt, in der Regel innerhalb von Deutschland. Die Unterauftragnehmer für die Infrastruktur und Plattformleistungen sind jeweils zertifiziert (z.B. DIN ISO/IEC 27001).

4.2 Aus rechtlichen Gründen ist es nicht möglich, Details zu den technischen und organisatorischen Maßnahmen der Unterauftragnehmer unmittelbar gegenüber dem Auftraggeber offenzulegen. Eine Offenlegung gegenüber dem Auftraggeber bedarf der vorherigen Unterzeichnung einer Geheimhaltungsvereinbarung zugunsten des jeweiligen Unterauftragnehmers.

4.3 Die Verarbeitung im Auftrag erfolgt grundsätzlich innerhalb der EU, in der Regel innerhalb von Deutschland. Ist das ausnahmsweise nicht möglich, weil weisungsgemäß Daten gegenüber Empfängern in Drittländern offengelegt werden müssen, z.B. zur Aufrechterhaltung der Verfügbarkeit der Cloud Services im Supportfall, geschieht dies ausschließlich, wenn für das Drittland ein Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO besteht oder beim Empfänger der Daten im Drittland geeignete Garantien gemäß Art. 46 DSGVO in Form von Standardvertragsklauseln (SCC) oder verbindlicher interner Datenschutzvorschriften (Binding Corporate Rules, BCR) bestehen.

rocon software development GmbH
Neumühler Weg 14
66130 Saarbrücken

saarbruecken@rocongruppe.de
www.rocongruppe.de

Anhang 3: Technisch-organisatorische Sicherheitsmaßnahmen

1 Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.1 **Zutrittskontrollmaßnahmen zu Serverräumen**: Für die Auftragsdatenverarbeitung werden personenbezogene Daten auf unseren Servern in unserem Rechenzentrum am Standort in 27356 Rotenburg, Heinrich-Schelper-Str.2 gespeichert. Der fensterlose Serverraum ist durch elektronische Zutrittskontrolle vor unbefugtem Zutritt gesichert. Zutrittsberechtigt sind nur die Geschäftsführung und die designierten, hausinternen IT-Administratoren. Der Zutritt erfolgt über personifizierte RFID-Medien. Personenbezogene Daten werden nicht in externe Rechenzentren bzw. Clouds übertragen.

1.2 **Zutrittskontrollmaßnahmen zu Büroräumen:** Der Zugriff auf personenbezogene Daten erfolgt von Mitarbeiter-Clientarbeitsplätzen an unseren Standorten in Rotenburg, Leipzig, Saarbrücken, Glaubitz und Dessau. Der Zutritt zu den Arbeitsplätzen wird durch Personal in den Empfangsbereichen bzw. Pförtnerdiensten kontrolliert. Die Büros und Gebäude sind außerhalb der Geschäftszeiten verschlossen und durch einen externen Wachdienst kontrolliert. Es werden elektronische Schließ-Systeme mit personifizierten RFID-Medien eingesetzt. Für den Zutritt von Betriebsfremden Personen (Gäste) gibt es Zutrittsregelungen, die u.a. vorsehen, dass diese nur in Begleitung die Büros betreten dürfen.

1.3 **Zugangs- und Zugriffkontrollmaßnahmen:** Zugriffe auf Daten werden im Unternehmen durch definierte Freigabeprozesse geregelt, sowohl hinsichtlich der Vergabe von Benutzerkennungen und Zugriffsberechtigungen als auch bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen. Es gibt definierte, vorgegebene Passwortparameter mit Mindestanforderungen an Komplexität sowie zentrale Verzeichnisdienste, die den Zugriff und die Berechtigungen regeln und protokollieren. Externe Zugriffe werden durch mehrschichtige Sicherheitslösungen bestehend u.a. aus Firewalls, VPN, Antivirus- und Antispamsoftware geregelt und geschützt.

1.4 **Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und Endgeräten:** Nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten sowie mobile Datenträger werden unter Verwendung geeigneter Technischer Mittel vollständig zerstört und entsorgt. Daten werden auf Festplatten verschlüsselt und nur auf Geräten des Unternehmens gespeichert - private Geräte sind nicht erlaubt.

1.5 **Maßnahmen zur sicheren Datenübertragung:** In Fällen, wo Datentransfer über das Internet erfolgen muss, findet immer eine Verschlüsselung statt (z.B. mittels SSL oder SFTP über den Anbieter DomainFactory). Notwendige Zertifikate zur Verschlüsselung werden von der eigenen, internen IT sowie dem Anbieter DomainFactory vorgehalten und verwaltet.

1.6 **Maßnahmen zur Sicherung der Fernwartung:** Zur Fernwartung (Remote-Session) wird das Tool AnyDesk eingesetzt. Um eine Fernwartung zu ermöglichen, muss der Kunde zunächst eine 9-

stellige Nummer dem Supportmitarbeiter übermitteln. Nachdem der Supportmitarbeiter die Nummer zur Verbindung eingegeben hat, muss der Kunde die Fernwartung zusätzlich erlauben, ohne dieses Zutun ist eine Fernwartung nicht möglich. Anydesk verschlüsselt alle Verbindungen mit TLS 1.2. Das bedeutet, dass die Kommunikation der Rechner direkt stattfindet und nicht auf Servern von AnyDesk. Sollte AnyDesk irgendeine Veränderung dieser Verbindung feststellen, wird die Verbindung unverzüglich aus Sicherheitsgründen beendet.

2 Maßnahmen zur Sicherstellung der Verfügbarkeit

2.1 **Serverraum:** Der Serverraum ist fensterlos, klimatisiert, von Massivwänden umgeben und mit einer redundant ausgelegten Klimaanlage ausgestattet. Es besteht eine Einrichtung zur unterbrechungsfreien Stromversorgung und sämtliche Einrichtungen und Geräte werden regelmäßig gewartet und Funktionstests unterzogen.

2.2 **Backup- und Notfall-Konzept, Virenschutz:** Es existiert ein Backup- und Notfallkonzept mit täglicher Sicherung auf Festplatten. Sicherungen werden verschlüsselt sowohl vor Ort als auch an einem sicheren Ort außerhalb des Brandabschnittes aufbewahrt und werden regelmäßig auf Wiederherstellungsfunktionalität geprüft. Es existieren Prozesse sowohl zum Software- und Patchmanagement als auch für Notfallmaßnahmen. Unbefugte Zugriffe werden vorgebeugt durch Einsatz von Sicherheitslösungen wie: Antivirus, Anti Spam, Antispyware und Firewalls.

2.3 **Netzanbindung:** Das Unternehmen ist am Standort Rotenburg per Glasfasernetz eines Providers mit dem Internet verbunden. Das Unternehmen am Standort Saarbrücken ist redundant über VDSL Anschlüsse zweier Provider mit dem Internet verbunden. An beiden Standorten stellt das Unternehmen jedoch keine Leistungen über diese an Drittparteien zur Verfügung.

3 Maßnahmen zur Gewährleistung der Sicherheit

3.1 Die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen wird regelmäßig überprüft, bewertet und evaluiert. Hierzu gehört auch die regelmäßige Überprüfung der im Auftrag der rocon software development GmbH tätigen Unterauftragnehmer einschließlich der von den Unterauftragnehmern umgesetzten technischen und organisatorischen Maßnahmen. Die Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen ist wesentlicher Bestandteil eines bei der rocongruppe installierten Informationssicherheits-Managementsystems.