Datenschutzrechtliche Vereinbarung (nachfolgend auch Vertrag genannt) über die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung gemäß Art. 28 DSGVO)

zwischen

- nachfolgend „Auftraggeber“ -

und

COMAN Software GmbH
Lüderitzer Straße 3-5
39576 Stendal

- nachfolgend „Auftragnehmer/Auftragsverarbeiter“ -

- gemeinsam nachfolgend „Vertragspartner“ -

1. Gegenstand und Dauer der Vereinbarung
a) Der Auftrag umfasst folgende Leistung:

Entwicklung individueller Softwarelösungen, Hosting und Betrieb der Software COMAN beim Auftragnehmer bzw. Unterstützungsleistungen beim Aufsatz und Betrieb der Software COMAN beim Auftraggeber

b) Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und auf Grundlage dieses Vertrages im Sinne von Art. 28 DSGVO.

c) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

d) Der Vertrag wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist drei Monate zum Monatsende. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Zweck, Umfang und Art der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen
a) Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich zweckgebunden.

b) Der Zweck, der Umfang und die Art sind wie folgt (gemäß der Definition von Art. 4 Nr. 2 DSGVO):

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

- Beschäftigtendaten
- Interessenten- / Kundendaten

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

- Name, Vorname,
- Telefonnummer
- E-Mail-Adresse

Besondere Kategorien von personenbezogenen Daten (entsprechend der Definition von Art. 9 und 10 DSGVO):

- Es werden keine besonderen personenbezogenen Daten verarbeitet.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

a) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

b) Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

c) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

d) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format durch den Auftraggeber zu bestätigen.

e) Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt, vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

f) Der Auftragsverarbeiter ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragsverarbeiters

a) Weisungsberechtigte Funktionen des Auftraggebers sind: COMAN-Keyuser gem. den Ausführungen im On-Boarding-Dokument.

b) Für Weisung zu nutzende Kommunikationskanäle:

- per E-Mail an folgende Adresse: support@coman-software.com
- per Telefon an folgende Rufnummer: +49(0)3931-6862666

c) Weisungsempfänger beim Auftragsverarbeiter sind: Mitarbeiter des Application Center

d) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

e) Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragsverarbeiters

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen/Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

b) Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Dies gilt nicht für Sicherheitskopien (Backups), die zur Aufrechterhaltung des Betriebs notwendig sein können.

c) Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

d) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten: Die in Ziffer 4 genannte weisungsberechtigte Funktion.

e) Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

f) Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen.

g) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

h)Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

i) Der Verarbeitung von Daten im mobilen Arbeiten stimmt der Auftraggeber zu. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall durch den Auftragsverarbeiter sicherzustellen.

j) Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutz-rechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, über die im Voraus durch den Auftraggeber zu informieren ist. Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

k) Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz bestellt:
Unternehmen: - Kertos GmbH
Kontaktdaten: - datenschutz@coman-software.com

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

a) Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.

b) Der Auftragsverarbeiter sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern für Kerndienstleistungen (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

a) Die zukünftige Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragsverarbeiter **ohne gesonderte Genehmigung** des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DSGVO. Der Auftragsverarbeiter muss dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen zudem immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter.

b) Mit der Beauftragung der in Anlage 1 genannten Subunternehmen ist der Auftraggeber einverstanden.

8. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

a) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber nach den Art. 28 Abs. 3 Buchst. c) und Art. 32 DSGVO technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. 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 DSGVO zu berücksichtigen.

b) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 2 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorweg mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nie unterschritten werden. Alle wesentlichen Änderungen sind zu dokumentieren. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

c) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

a) Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, durch mehrmaliges (mind. dreifaches) Überschreiben des Datenträgers mit Ziffern und Zeichen zu löschen.

b) Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Sonstiges

a) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

b) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Dies gilt auch für eine Änderungen des Formerfordernisses.

c) Als Gerichtsstand wird das für den Auftragsverarbeiter örtlich zuständige Gericht vereinbart.

d) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich zu verständigen.

e) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

f) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Auftraggeber

Name

Ort, Datum

Unterschrift

Auftragnehmer/Auftragsverarbeiter

Timur Ripke, Sven Kägebein
Name

Stendal,
Ort, Datum

Unterschrift

Anlage 1 – Technische und organisatorische Maßnahmen / Datenschutzkonzept

Transparenz

- Dokumentation erforderlicher Datenschutzfolgeabschätzungen (DSFA)
- Einwilligungserklärung zu Bild-, Ton- und Videoaufnahmen (Aufzeichnung Web-/Videokonferenz)
- Die Datenempfänger der Verarbeitungstätigkeiten sind gesetzeskonform dokumentiert
- Die Art, der Umfangs, die Umstände und die Zwecke der Verarbeitung sind gesetzeskonform nach Art. 30 DSGVO dokumentiert
- Sorgfältige Auswahl des Auftragnehmers (Auftragskontrolle / Sicherheit der Verarbeitung)
- Erlaubnisbasiertes Verfahren – Double-Opt-In-Verfahren (DOI)
- Prozess für auskunftsersuchenden Betroffenen
- Dokumentation verbindlicher Löschfristen
- Signal-Hinweis und Funktionsbeschreibung für Anlagen und Anwendungen zur Aufschaltung auf laufende Gespräche (Mithören) – Telefonanlagen (TK-Anlage)
- Dokumentation von Auftrags- und Unterauftragsverhältnissen

Zweckbindung

- Entgegennehmen von Weisungen nur von befugten Mitarbeitern des Verantwortlichen bzw. Auftraggebers
- Verpflichtung der Mitarbeiter auf die Beachtung der Anforderungen der DSGVO
- Im Verzeichnis der Verarbeitungstätigkeiten ist der Zweck der Verarbeitung korrekt gepflegt

Datenminimierung

- Video Hosting auf der eigenen Website – Einbindung eigener Videos
- Datenschutz wird durch datenschutzfreundliche Gestaltung der Technik (Privacy-by-Design) von Produkten und Leistungen umgesetzt
- Festlegung verbindlicher Löschfristen (Löschkonzept)
- Regelmäßige Audits über den Umfang der verarbeiteten Daten durch den Datenschutzbeauftragten

Richtigkeit

- Captcha-Dienst / Spam-Prävention für Websites
- Personen werden bei Anfragen zu personenbezogenen Daten korrekt identifiziert
- Dokumentation zum Nachweis der Datenherkunft
- Es besteht ein geregelter Prozess zur zentralen Verwaltung (Änderung) von Benutzeridentitäten (Benutzerkennung)
- Unverzügliche Löschung unrichtiger und nicht korrigierbarer Daten

Vertraulichkeit - Zutrittskontrolle

- Protokollierung und Auswertung der Zugangskontrolle
- Physisches Schließsystem (Sicherheitsschlösser)
- Wachpersonal (Patrouille)
- Diebstahl- und Einbruchsschutz für Räume der technischen Infrastruktur
- Einbruchmelder - Zutrittskontrolle
- Zutrittskontrolle zu Servern (Räumliche Gegebenheiten Büro, Kanzlei, Praxis)
- Einsatz eines Intrusion-Prevention-Systems

- Nutzung von Blickschutzfiltern bei mobilen Geräten in öffentlichen Räumen (Personennahverkehr, Hotels, Restaurants)
- Netzwerk mit demilitarisierter Zone (DMZ)
- Elektronisches Schließsystem (Sicherheitsschlösser mit Codesperren)
- Es sind Sicherheitsüberwachungssystem in den Bereichen vorhanden, in denen personenbezogene Daten verarbeitet werden
- Führen eines Schlüsselbuchs (Dokumentation der Zutrittskontrolle)
- Jeder Nutzer der IT verfügt über eine individuelle Benutzerkennung
- Umsetzung von Sicherheitszonen und klaren Zutrittsbefugnissen
- Auswahl von Reinigungs- und Wachpersonal und Verpflichtung zur Vertraulichkeit und Verschwiegenheit
- Datenverarbeitungsanlagen (z. B. Server) sind sicher im Sicherheitskäfig bzw. Sicherheitsschrank verwahrt
- Die Abmeldung von Systemen (z. B. Windows oder Websoftware) von Nutzern erfolgt automatisch nach einem definierten Zeitraum (Time-Out) bzw. der Zugriff auf den Computer wird durch Sperrung beschränkt.
- Besuchermanagement (Anmeldung/ Empfang/Begleitung)
- Zutrittskontrolle zu Räumen der Datenverarbeitung
- Videoaufzeichnungen definierter Bereich
- Reinigungszeiten während der Arbeitszeit unter Aufsicht
- Sicherung des Raumes der Datenverarbeitungsanlagen
- Regelung zur Sperrung von Zugängen ausscheidender Mitarbeiter (Offboarding)
- Besuchermanagement (Anmeldung/ Empfang/Begleitung)

Vertraulichkeit - Zugangskontrolle

- Umsetzung von Rollen- und Rechtemanagement (Rollen- und Berechtigungskonzept)
- Home-Office / Telearbeit: Vertraulichkeit bei Telefon- und Videokonferenzen
- Benutzer (sind angewiesen) den Computer beim Verlassen des Arbeitsplatzes zu sperren (Bildschirmsperre)
- Nutzung sicherer Datenübermittlungsverfahren, die eine Manipulation versendeter Daten verhindern (z.B. DE-Mail, VPN, verschlüsselte Mails, verschlüsselte Dateien)
- Verfahren zur Authentifizierung–Authentifikation mittels Passworteingabe oder biometrischer Scans
- Firewall-Lösung als Cloud-Service (Einsatz Security-Stack)
- Der Zugriff auf Verzeichnisdienste (z. B. Dateien auf einem gemeinsamen Server) ist durch Authentifizierungsmaßnahmen (Username + Passwort) beschränkt.
- Einsatz einer Firewall zum Schutz des internen Netzwerkes
- Regelung zur Einrichtung von Zugängen neuer Mitarbeiter in die digitalen Systeme des Unternehmens (Onboarding-Prozess)
- Zugangskontrollsystem (ZKS)
- Benutzer (sind angewiesen) den Computer beim Verlassen des Arbeitsplatzes zu sperren (Bildschirmsperre)
- Passwortrichtlinie (Kennwortrichtlinie)
- Zwei-Faktor-Authentisierung (2FA) wird wenn möglich zum Login angewendet

Vertraulichkeit - Zugriffskontrolle

- Managed Print Services (MPS)/Geräte- und Dokumentenmanagement (Monitoring)

- Administratorrechte sind auf verschiedene Personen aufgeteilt, Super-Administratoren werden möglichst vermieden
- Home-Office / Telearbeit: Gewährleistung der Dokumentensicherheit / Lagerung und Verschluss von Papierunterlagen
- Verpflichtung zur Wahrung des Datengeheimnisses und Verschwiegenheitserklärung
- Minimierung von Administratorzugängen
- Mobile-Device-Management im Einsatz
- Trennung von Test- und Produktivsystemen
- Home-Office / Telearbeit: Umgang mit Papierdokumenten (Risiken der Schädigung)
- Delegation von Benutzerrechten und Programmberechtigungen – Rollen- und Rechtemanagement
- Einsatz von Dateiverschlüsselung
- Die sichere Vernichtung personenbezogener Daten in Papierform ist gewährleistet.
- Protokollierung von Anmeldevorgängen
- Verwendung privater Hardware (BYOD)
- Zugriffskontrolle zur Benutzung eines Datenverarbeitungssystems
- Sichere Internetverbindung/Verschlüsselung im Internet (SSL, TLS)
- Verschlüsselte Nutzung eines WLAN für Bürotätigkeiten
- Ein Plan zum Patch Management ist vorhanden und ist fester Bestandteil der IT-Organisation.
- Einsatz von Datenträgerverschlüsselung
- Identitätsmanagement (IdM) und Identity and Access Management (IAM oder IdAM)
- Einsatz von Mailverschlüsselung
- Einsatz von VPN-Netzwerk
- Deaktivierung nicht benötigter Netzwerk-Ports (Netzwerksicherheit / Serversicherheit)
- Enterprise Mobility Management (EMM)
- Aufbewahrung mobiler Speichermedien bei Nichtgebrauch
- Schutz von Betriebs- und Geschäftsgeheimnissen
- Datenklassifizierung

Integrität

- Kabelgebundener Netzwerkzugang: Network Admission Control
- Einsatz von Betriebssystemen und Sicherheits-Updates
- Schutzmaßnahmen zur sicheren Nutzung von E-Mail-Diensten (E-Mail-Sicherheit bei Spam, Malware und Phishing)
- Auswahl und Einsatz von (Standard-)Software
- Barrierefreie PDF (Barrierefreie Gestaltung von Internetangeboten)
- Weitergabekontrolle durch Einrichtungen der Datenübertragung
- Verschlüsselung von Datenbanken
- Dokumentenmanagement mit Versionierungssystem
- E-Mail-Gateway mit Filterfunktionen
- Eingabekontrolle bei Datenverarbeitungssystemen
- Übergabepunkte und Ladezonen sind von den Räumen, in denen die Datenverarbeitungsanlagen untergebracht sind, separiert.
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von Virenschutzlösung/ Regelmäßige Aktualisierung des Virenschutzprogramms
- Externe Dateien und Ordner auf Viren untersuchen (Online-Virenscanner / Antivirenprogram)

Verfügbarkeit

- Regelungen für die Durchführung der Datensicherungen (Backups)
- Instandhaltung Technischer Anlagen und Komponenten (Ausfallsicherheit)
- Sicherstellung der Langzeitarchivierung und Verfügbarkeit durch Umspeicherung verschlüsselter Daten auf andere Datenträger zur Gewährleistung der Prüf- und Lesbarkeit
- Vertretungsregelung Administrator
- Versorgungsleitungen (Strom, Breitband, Gas, Wasser, sonst. Meldeleitungen)
- Verringerung der Brandlasten im Raum der Datenverarbeitung
- Verantwortliche (z. B. Admins) werden durch automatisierte Alarmsysteme über einen System-Ausfall informiert
- Weitestgehender Verzicht auf Makros in Office-Dokumenten
- Zugriffsrechte orientieren sich an Zuständigkeiten
- Wartung der IT-Infrastruktur (Ausfallsicherheit)
- Sicherheits-Stromversorgung/Notstromanlagen (Notstrom-Systeme)
- Verfügbarkeitskontrolle bei der Verarbeitung personenbezogener Daten
- Stromkreise
- Unterbrechungsfreie Stromversorgung (USV)
- Das Klima der Räume in denen Datenverarbeitungsanlagen (z. B . Serverraum) stehen werden klimatisch überwacht und das Klima wird (automatisiert) geregelt.
- Auto-Start von externen Medien ist deaktiviert, die Verwendung externer Medien erheblich eingeschränkt.
- Die IT-Systemlandschaft ist umfangreich dokumentiert
- Dokumentation des Datenschutz-Management-Systems (DSMS) in der Robin Data Software
- Einsatz von Content Management Systemen (CMS)
- Festgelegte Zuständigkeiten im Rahmen der Datensicherung
- Feuerlöscher sind für die Räume der Datenverarbeitungsanlage vorhanden
- Gefährdungsschutz (Naturkatastrophen) für Rechenzentrum (RZ) sowie Serverraum
- Festplattenvollverschlüsselung bei PCs und Notebooks (Hardwaregestütze Verschlüsselung)
- Dokumentation des Datenschutz-Management-Systems (DSMS) in der Robin Data Software
- Rauchmeldeanlagen im Raum der Datenverarbeitungsanlagen
- Raum der Datenverarbeitungsanlagen ist klimatisiert
- Penetration Tests (Schwachstellenanalyse - Penetration IT-System, Webseite, Cloudlösungen)
- Personalrisiken erkennen und begegnen (Personalrisikomanagement)

Belastbarkeit

- One-Premise-Lastenausgleich der Server
- Lastenausgleich der Netzwerkkomponenten
- Lastenausgleich für SaaS-Lösungen
- Bei hochverfügbaren Lösungen erfolgt ein Cloud-basierter Lastenausgleich per virtualisierten Server, die in einem sicheren Land gehostet werden.
- Installation verfügbarer Sicherheitsupdates
- Überspannungsschutz
- Die Räume mit den Datenverarbeitungsanlagen sind baulich geeignet (z. B. Lambertz-Zelle, nicht im feuchten Keller, vor unbefugtem Zutritt geschützt).

Rechenschaftspflichten

- Bei Anbietern von Videokonferenzsystemen in unsicheren Drittstaaten sind geeignete Garantien vorhanden.
- Zugriff und Auswertung der Aufzeichnungen der Videoüberwachung
- Vertretungsregelung Datenschutzbeauftragter
- Administration der Videoüberwachung - Privacy by default (Datenschutzfreundliche Voreinstellungen)
- Bei Videokonferenzen kann der Hintergrund eines Nutzers softwareseitig unscharf gestellt werden (Blurring)
- Auftragskontrolle bei der Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung / AV-Vertrag)
- Dienstlich zur Verfügung gestellte Geräte werden nicht für private Zwecke genutzt.
- Die Tätigkeiten der Datenschutzzuständigen werden dokumentiert
- Zugriff und Auswertung der Aufzeichnungen der Videoüberwachung
- Administration der Videoüberwachung - Privacy by default (Datenschutzfreundliche Voreinstellungen)
- Ein Datenschutzbeauftragter (extern) ist bestellt und kann weisungsfrei agieren.
- Dokumentation Erste-Hilfe-Maßnahmen (Organisation des Arbeitsschutzes)
- Prozess der Meldung einer Datenschutzverletzung (Datenpanne)
- Regelmäßige Audits zur Überprüfung der Wirksamkeit der Datenschutzmaßnahmen
- Regelmäßige Auswertung und Prüfung der Serverprotokolle
- Netztrennung zwischen den WLAN-Netzen – Maßnahmen für einen sicheren WLAN-Betrieb
- Täglich Updates der Virensignaturen auf den Clients sind gewährleistet.
- Festlegung und Kommunikation der Zuständigkeiten im Update- und Patchmanagement
- Home-Office / Telearbeit: Einsatzplanung im Home Office (Mitarbeiterübersicht)
- Kontinuierliche Aktualisierung des Datenschutz-Management-Systems (DMS)
- Führen des Verzeichnisses der Verarbeitungstätigkeiten (Verfahrensverzeichnis)
- Entfernung von Eigentum des Unternehmens
- Regelmäßig dokumentierte Schulungen der Mitarbeiter auf den Datenschutz.
- Digitales Equipment wird vom Arbeitgeber gestellt
- Dokumentation getroffener Sicherheitsmaßnahmen (VV, TOMs)
- Eine Datenschutzorganisation ist in der Organisation etabliert (mit oder ohne DSB)
- Dokumentation der vorhandenen IT-Infrastruktur und der Schutzbedarfe
- Die automatische Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten wird durch die Konfiguration unterbunden.

Nicht-Verkettung

- Logische Mandantentrennung
- Trennungsgebot bei der Verarbeitung personenbezogener Daten

Anlage 2 – Subunternehmen

Dienstleister	**Dienstleistung**	**Ort der Datenverarbeitung**
Cronon GmbH	Rechenzentrum	Deutschland
Microsoft Corporation	Microsoft 365 (Office-Anwendungen und Kommunikation)	Europa
Atlassian. Pty Ltd	**J**ira (Ticketsystem)	**G**lobal
HubSpot, Inc.	CRM und Websitehosting	Europa
TeamViewer Germany GmbH	TeamViewer (Remotezugriff)	Deutschland
RealtimeBoard Inc. dba Miro	Miro (Projektplanung)	Global

Dokumentenhistorie

Version	Datum	Autoren	Änderung
1.0	07.04.2018	H. Fierdag	INIT
1.1	12.06.2021	H. Fierdag	Aufnahme & Erweiterung TOM‘s
1.2	03.11.2023	Y. Hoffmann	Aktualisierung TOM’s & Dienstleister
1.3	29.12.2024	Y. Hoffmann	Aktualisierung TOM’s & Dienstleister