# Anlage 2[1]

# Vereinbarung zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO

[1]Anlage 2, Vereinbarung zur Auftragsvereinbarung, ist integraler Bestandteil Vers. 2 – 01/26 RTC Nutzerungsvereinbarung-Vertrag.

## Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag / der Beauftragung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten. Konkret geregelt werden in dieser Vereinbarung zur Auftragsverarbeitung Tätigkeiten der zentralen Services für die Unternehmensfamilie.

## § 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag oder dem Auftrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die in Anlage 1 aufgeführten Daten Bestandteil der Datenverarbeitung. Sofern diese im Vertrag bereits geregelt sind, versteht sich die Angabe in Anlage 1 lediglich zu Informationszwecken.

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung und der Anlage 1 zu dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

## § 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag, in der Beauftragung und/oder in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

## § 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz--Grundverordnung (Art. 32 DS-GVO) genügen.

Der Auftragnehmer hat 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. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die vom Auftragnehmer etablierten Maßnahmen sind in Anlage 2 dieser Vereinbarung zur Auftragsdatenverarbeitung aufgeführt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass jegliche Sicherheitsmaßnahmen dem Stand der Technik entsprechen sowie das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Die Kontaktdaten sind in Anlage 1 dieser Vereinbarung aufgeführt.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(11) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

## § 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Die Kontaktdaten sind in Anlage 1 dieser Vereinbarung aufgeführt.

## § 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

## § 6 Nachweismöglichkeiten und Kontrollrechte

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Diese werden zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine angemessene Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer und Auftraggeber grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

## § 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Die zum Zeitpunkt des Abschlusses dieser Vereinbarung tätigen Subunternehmer sind in Anlage 1 aufgeführt. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber (ggf. Frist und/oder Regelung für Notfallsituationen). Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber und dem Auftragnehmer ein Sonderkündigungsrecht eingeräumt.

(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

(4) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. verbundene Unternehmen mit den aufgeführten Leistungen unterbeauftragt. Absatz 3 gilt entsprechend auch für verbundene Unternehmen.

## § 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

## § 9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

**Anlage 1**

**Auftragsgegenstand**

Der Auftragsgegenstand umfasst:
Bereitstellung eines definierten Speicherplatzes auf einem Server zur Speicherung von Kundendaten

**Dauer der Beauftragung**

Die Dauer der Beauftragung richtet sich nach der Vertragsdauer der Nutzungsvereinbarung

**Art der Daten**

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien:
Personenstammdaten (Namen, Benutzernamen, Aliase)
Kommunikationsdaten (E-Mail-Adressen, Telefonnummern)
Protokoll- und Logdateien

**Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
Benutzer des Portals

**Subunternehmer**

| **Name und Anschrift** | **Kurzbeschreibung der Tätigkeit** |
|---|---|
| Modern Drive Technology GmbH<br>Rettichstraße 7<br>92318 Neumarkt in der Oberpfalz | Bereitstellung eines definierten Speicherplatzes auf einem Server zur Speicherung von Kundendaten |

**Datenschutzbeauftragter beim Auftragnehmer**

| **Name** | **Anschrift & Kontakt** |
|---|---|
| Markus Olbring<br>externer Datenschutzbeauftragter | comdatis it-consulting<br>Deventer Weg 8, 48683 Ahaus<br>Telefon: 02561-7569986 oder 0173-9799897<br>Mail: datenschutz@ruthmann.de |

*Sofern keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten vorliegt, ist ein Ansprechpartner für Datenschutzfragen zu benennen.

**Anlage 2**

| Beschreibung | Maßnahme | ja | nein | nicht relevant |
|---|---|---|---|---|
| Zutrittskontrolle | Das Unternehmen verfügt über einen zentralen und besetzten Empfangsbereich. | x | | |
| | Ein Zutrittskontrollsystem ist im Unternehmen vorhanden, d.h. Türsicherung durch Türöffner, Ausweisleser, Schließautomatik o.ä. | x | | |
| | Die Räumlichkeiten des Unternehmens sind stets verschlossen. | | x | |
| | Es existiert eine Zutrittsregelung für betriebsfremde Personen. | x | | |
| | Im Unternehmen ist eine zentrale Schlüsselverwaltung zur Ausgabe von Schlüsseln etabliert. | x | | |
| | An zentraler Stelle wird eine Schlüsselliste geführt, aus der hervorgeht, welcher Mitarbeiter wann einen Schlüssel erhalten hat. | x | | |
| | Mitarbeiter wurden schriftlich dazu verpflichtet, den Verlust eines Schlüssels umgehend zu melden. | x | | |
| | Besucher erhalten einen Besucherausweis und geben diesen bei Verlassen des Unternehmens zurück. | | x | |
| | Der Zutritt zu Serverräumen ist auf berechtigte Mitarbeiter beschränkt. | x | | |
| | Serverräume sind stets verschlossen. | x | | |
| | Es erfolgt eine Protokollierung der Zutritte zu Serverräumen. | x | | |
| | Das Gebäude ist alarmgesichert. | | x | |
| | Das Gebäude befindet sich auf einem umzäunten Gelände. | x | | |
| | Eine Gebäudeüberwachung erfolgt durch Video, Werkschutz oder Nachtwächter/Wachdienst. | x | | |
| Zugangskontrolle | Mitarbeiter erhalten individuelle Benutzernamen und Kennwörter für die Anmeldung am PC-Arbeitsplatz. | | x | |
| | Initialkennwörter müssen vom Anwender geändert werden. | x | | |
| | Kennwörter müssen regelmäßig geändert werden. | x | | |
| | Kennwörter verfügen über Komplexitätsanforderungen (z.B. Zahlen, Buchstaben, Sonderzeichen). | x | | |
| | Kennwörter sind mindestens 8 Zeichen lang. | x | | |
| | Administrative Kennwörter sind mindestens 12 Zeichen lang. | x | | |
| | Alternativ zu regelmäßigen Kennwortänderungen befinden sich Verfahren einer Zwei-Faktor-Authentifizierung im Einsatz. | x | | |
| | PC-Arbeitsplätze werden bei Inaktivität automatisch gesperrt und können nur durch Kennworteingabe wieder entsperrt werden. | x | | |
| | Interne Netze sind gegen unberechtigte Zugriffe von extern durch eine Firewall geschützt. | x | | |
| | Externe Zugriffe auf interne Netze sind ausschließlich über verschlüsselte Verbindungen (z.B. VPN) möglich. | x | | |
| | Datenträger von mobilen Endgeräten (Notebooks, Smartphones, Tablets), auf denen sich personenbezogene Daten befinden, sind verschlüsselt. | x | | |
| | PC-Arbeitsplätze und Notebooks verfügen über einen Anti-Viren-Schutz. | x | | |

| | | | | |
|---|---|---|---|---|
| Zugriffskontrolle | Ein Berechtigungskonzept liegt im Unternehmen vor und enthält differenzierte Berechtigungsstufen. | | x | |
| | Über Benutzerprofile ist in den Anwendungen sichergestellt, dass Mitarbeiter ausschließlich die Rechte erhalten, die zur Aufgabenerfüllung notwendig sind. | x | | |
| | USB-Anschlüsse an den PC-Arbeitsplätzen sind gesperrt bzw. unterliegen einer technischen Überwachung. | x | | |
| | Brenner an den PC-Arbeitsplätzen sind gesperrt bzw. unterliegen einer technischen Überwachung. | x | | |
| | Mitarbeiter sind dazu verpflichtet, ausschließlich vom Unternehmen ausgegebene externe Datenträger zu verwenden. | x | | |
| | Nicht mehr benötigte IT-gestützte Datenträger werden datenschutzgerecht entsorgt. | x | | |
| | Administrative Rechte stehen ausschließlich für berechtigte Mitarbeiter zur Verfügung. | x | | |
| Trennungsgebot | Zu unterschiedlichen Zwecken erhobene personenbezogene Daten werden getrennt gespeichert. | x | | |
| | Die Anwendungen erlauben eine logische Mandantentrennung. | x | | |
| | Eine Mandatentrennung ist über das implementierte Berechtigungskonzept implementiert. | x | | |
| | Im Unternehmen wird zwischen Produktiv- und Testsystem unterschieden. | x | | |
| | Daten unterschiedlicher Projekte / Auftraggeber werden, soweit möglich, getrennt verarbeitet. | x | | |
| | Bei pseudonymisierten Daten ist gewährleistet, dass eine Trennung der Zuordnungsdatei zu den Daten vorliegt. | | x | |
| Weitergabekontrolle | Im Unternehmen stehen Verfahren zu Verfügung, die einen verschlüsselten Austausch personenbezogener Daten ermöglichen (z.B. E-Mail-Verschlüsselung, SFTP, https). | x | | |
| | Beim Versand personenbezogener Daten (z.B. per Mail) sind Mitarbeiter schriftlich dazu verpflichtet, diese Daten verschlüsselt zu versenden. | | x | |
| | Anhand einer Arbeitsanweisung, Betriebsvereinbarung oder Richtlinie wurden Mitarbeiter dahingehend verpflichtet, personenbezogene Daten keinesfalls über unsichere oder nicht datenschutzkonforme Dienste auszutauschen (z.B. keine Datenweitergabe über Social Media, WhatsApp, privat verwendete oder kostenlose Cloud-Speicherdienste). | x | | |
| Eingabekontrolle | Eine Nachvollziehbarkeit von Eingabe, Änderung und Löschung von personenbezogenen Daten ist systemseitig durch eine Protokollierung (Wer? Wann?) gegeben. | | x | |
| | Bei Einsatz von Standardsoftware ist sichergestellt, dass ausreichende und den Datenschutzanforderungen entsprechende Protokollierungen aktiviert sind. | | x | |
| Verfügbarkeitskontrolle | Ein dokumentiertes Notfallkonzept ist im Unternehmen vorhanden. | x | | |
| | Es werden regelmäßig Notfallübungen durchgeführt. | | x | |
| | Es erfolgt eine redundante Absicherung von Servern und Datenbeständen. | x | | |
| | In den Serverräumen liegt eine angemessene unterbrechungsfreie Stromversorgung (USV) vor. | | x | |

| | | | | |
|---|---|---|---|---|
| | Die Serverräume verfügen über redundante Klimaanlagen. | x | | |
| | Die Serverräume verfügen über Rauchmelder. | x | | |
| | Im oder vor den Serverräumen befinden sich Feuerlöscheinrichtungen. | x | | |
| | Die Serverräume verfügen über einen Sensor für die Alarmanlage. | | x | |
| | Es erfolgen Alarmmeldungen bei unberechtigten Zutritten zu Serverräumen. | | x | |
| | Datensicherungen werden an einem sicheren, ausgelagerten Ort aufbewahrt. | x | | |
| | Datenrücksicherungen erfolgen regelmäßig durch Testszenarien. | | x | |
| | Virenscanner sind unternehmensweit auf den Endgeräten installiert. | x | | |
| | Virenscanner aktualisieren sich automatisch. | x | | |
| | Betriebssysteme auf Client-Arbeitsplätzen werden regelmäßig aktualisiert. | x | | |
| | Betriebssysteme auf Servern werden regelmäßig aktualisiert. | x | | |
| | Im Unternehmen sind Verfahren implementiert, die eine regelmäßige Aktualisierung auch für Hilfsprogramme (z.B. PDF-Reader, ZIP-Programme, Java, Flash) gewährleisten. | | x | |
| | Im Unternehmen gibt es verbindliche Richtlinien für die Wartung und Durchführung von Updates | | x | |
| | Durch ein automatisches und permanentes Monitoring zur Erkennung von Störungen werden etwaige Fehler schnell gemeldet. | x | | |
| | Kritische IT-Systeme im Unternehmen, insbesondere solche mit Erreichbarkeit über das Internet, werden Schwachstellentests unterzogen. | | x | |
| | Die Firewall- und Routersysteme werden regelmäßig aktualisiert (Firmwareupdate). | x | | |
| Auftragskontrolle | Die Auswahl von externen Dienstleistern erfolgt unter Anwendung größter Sorgfalt (insbesondere bezüglich des Datenschutzes und der Informationssicherheit). | x | | |
| | Beim Einsatz externer Dienstleister ist sichergestellt, dass eine Datenverarbeitung nicht außerhalb der EU oder einem sicheren Drittland erfolgt. | x | | |
| | Mit externen Dienstleistern, die personenbezogene Daten verarbeiten oder im Rahmen der Tätigkeit einsehen könnten, bestehen vertragliche Regelungen unter Einhaltung der Vorgaben aus Art. 28 der Datenschutzgrund-Verordnung. | x | | |
| | Beim Einsatz externer Dienstleister, die personenbezogene Daten verarbeiten, wird sichergestellt, dass eine Rechtsgrundlage für die Verarbeitung (z.B. Vereinbarung zur Auftragsdatenverarbeitung, EU-Standardvertragsklauseln) gegeben ist. | x | | |
| | Es sind Verfahren implementiert, die sicherstellen, dass personenbezogene Daten nach Auftragsende vernichtet bzw. gelöscht werden. Etwaige gesetzliche Aufbewahrungsfristen werden dabei berücksichtigt und eingehalten. | x | | |
| | In den vertraglichen Regelungen mit externen Dienstleistern werden Kontrollrechte vereinbart. | x | | |
| | Die vereinbarten Kontrollrechte werden in regelmäßigem Abstand geltend gemacht (z.B. durch Einholung einer Bestätigung, eines Berichtes) | | x | |

| | | | | |
|---|---|---|---|---|
| | Externe Dienstleister werden zur Verschwiegenheit verpflichtet. | x | | |
| Datenschutzmanagement | Ein Datenschutzbeauftragter ist im Unternehmen schriftlich bestellt. | x | | |
| | Es besteht keine gesetzliche Verpflichtung zur Bestellung eines Datenschutzbeauftragten. | | | x |
| | Durch eine Leitlinie zum Datenschutz und zur Informationssicherheit hat die Geschäftsleitung alle Mitarbeiter über die Notwendigkeit des Datenschutzes informiert. | x | | |
| | Im Unternehmen bestehen schriftliche Vorgaben (z.B. Richtlinie, Betriebsvereinbarungen) für den Umgang mit Daten und den IT-Systemen. | | x | |
| | Mitarbeiter sind schriftlich zur Verschwiegenheit verpflichtet. | x | | |
| | Mitarbeiter werden in Schulungen bezüglich des Datenschutzes sensibilisiert. | | x | |
| | Im Unternehmen liegt ein dokumentiertes Verzeichnis der Verarbeitungstätigkeiten vor. Darin werden, sofern notwendig, auch Verarbeitungstätigkeiten im Auftrag dokumentiert. | x | | |
| | Im Unternehmen liegt eine Dokumentation der Maßnahmen zur Sicherheit der Verarbeitungstätigkeiten vor (sog. TOM's) | | x | |
| | In regelmäßigen Prüfungen wird sichergestellt, dass die etablierten Maßnahmen zur Einhaltung des Datenschutzes angemessen sind. | | x | |
| | Der Datenschutzbeauftragte erstellt einen jährlichen Bericht. | x | | |
| | Im Unternehmen liegt eine Zertifizierung im Bereich der Informationssicherheit vor (z.B. ISO/IEC 27001, IDW PS 951, VdS 3473). | | x | |
| | Im Unternehmen liegt eine Zertifizierung im Bereich des Datenschutzes vor. | | x | |