Vereinbarung zum Datenschutz

Der Auftragnehmer

rocon Rohrbach EDV-Consulting GmbH

Isaac-Fulda-Allee 1

55124 Mainz

verarbeitet im Auftrag des Auftraggebers (auch „Verantwortlicher“) personenbezogene Daten im Rahmen einer Auftragsdatenverarbeitung gemäß Art. 28 EU Datenschutz-Grundverordnung (DS-GVO).

Diese Vereinbarung gilt für alle Vertragsverhältnisse zwischen den Parteien, in denen auf diese Vereinbarung Bezug genommen wird. Der Auftraggeber ist in dem jeweiligen zwischen den Parteien geschlossenen Einzelvertrag („Hauptvertrag“) näher definiert. Die Einzelheiten der vertraglichen Vereinbarungen zwischen den Parteien sind in dem zwischen den Parteien geschlossenen Hauptvertrag zur Beauftragung der jeweiligen Leistung festgelegt.

Für diese Datenvereinbarung im Auftrag des Verantwortlichen vereinbaren die Parteien Folgendes:

§ 1. Gegenstand der Vereinbarung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Gegenstand, Art und Zweck der Verarbeitung personenbezogener Daten ergeben sich aus dem Hauptvertrag zwischen dem Auftraggeber und dem Auftragnehmer, sowie den darin in Bezug gesetzten Leistungsbeschreibungen der Leistungen des Auftragnehmers durch den Auftragnehmer sowie den zusätzlichen Hinweisen hierzu in Anlage 1.

(2) Die vom Auftrag betroffenen Personen und die damit verbundenen Zugriffe auf deren Daten sowie die Art der personenbezogenen Daten sind in Anlage 2 aufgeführt.

(3) Die Dauer dieses Auftrags entspricht der Laufzeit des Hauptvertrags und der darin enthaltenen Leistungsvereinbarung (siehe auch Anlage 1). Die Verpflichtungen zur Einhaltung des Datengeheimnisses und der Vertraulichkeit bestehen auch nach Beendigung dieser Vereinbarung fort.

(4) Änderungen des Verarbeitungsgegenstandes, Verarbeitungsumfanges sowie Verfahrensänderungen sind schriftlich zu vereinbaren.

(5) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DS-GVO erfüllt sind.

§ 2. Pflichten des Auftragnehmers

(1) Der Auftragnehmer führt die Leistungen ausschließlich im Rahmen der getroffenen Vereinbarung und nach Weisung des Auftraggebers durch. Der Auftragnehmer ist verpflichtet, die getroffenen Weisungen unverzüglich zu dokumentieren. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen geltendes Recht verstößt.

(2) Der Auftragnehmer verwendet Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, nur für die vereinbarten Vertragszwecke. Eine Verarbeitung oder Nutzung ohne Kenntnis des Auftraggebers oder zu eigenen Zwecken des Auftragnehmers ist nicht erlaubt. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend Art. 32 DS-GVO zu. Die konkreten Vorgaben sind durch Anlage 3 geregelt. Die Parteien sind sich darüber einig, dass die in Anlage 3 dargestellten technischen und organisatorischen Sicherheitsmaßnahmen ein angemessenes Sicherheitsniveau für die Auftragsverarbeitung sicherstellen. Der Auftragnehmer kann die technischen und organisatorischen Maßnahmen ändern, sofern dadurch mindestens das gleiche Maß an Sicherheit für die personenbezogenen Daten des Verantwortlichen gewährleistet ist.

(4) Der Auftragnehmer hat einen Datenschutzbeauftragten (DSB) benannt, der in Anlage 4 aufgeführt ist. In den Datenschutzhinweisen auf der Website des Auftragnehmers (https://www.rocon.info/datenschutz) wird der jeweils aktuelle DSB aufgeführt.

(5) Der Auftragnehmer verpflichtet sich, soweit rechtlich und tatsächlich möglich, den Verantwortlichen auch mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen zu unterstützen, die Betroffene zur Ausübung ihrer Rechte nach Art. 12-22 DS-GVO stellen. Dies betrifft insbesondere das Auskunftsrecht der Betroffenen (Art. 15 DS-GVO), das Recht auf Berichtigung unrichtiger personenbezogener Daten, das Recht der Betroffenen auf Löschung ihrer personenbezogenen Daten (Art. 17 DS-GVO) sowie das Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO). Der Auftragnehmer darf Daten nur auf dokumentierte Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Er wird ferner keinerlei Auskunft über personenbezogene Daten an Dritte, aber auch nicht an den Betroffenen selbst erteilen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(6) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit schriftlich verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(7) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers sowie in Fällen eines Verstoßes gegen die in diesem Auftrag getroffenen Festlegungen. Ebenso informiert er den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde oder anderer öffentlicher Stellen, die sich auf die Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung auswirken.

(8) Darüber hinaus unterstützt der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei seinen Verpflichtungen aus Art. 33 DS-GVO (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) sowie aus Art. 34 DS-GVO (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person). Ebenso unterstützt er den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Durchführung der Datenschutz-Folgenabschätzung, einer ggf. erforderlichen Konsultation der Aufsichtsbehörde (Art. 35, 36 DS-GVO) sowie sonstigen behördlichen Anfragen und Kontrollen. Soweit auf Seiten des Auftragnehmers bei der notwendigen Unterstützung Kosten entstehen, hat der Auftraggeber diese Kosten auf Grundlage der üblichen Tages-/Stundensätze des Auftragnehmers zu ersetzen, es sei denn, die Tätigkeiten sind aufgrund eines vom Auftragnehmer zu vertretenden Verstoßes gegen diese Vereinbarung oder gegen geltendes Gesetz zu ergreifen.

(9) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten, das den Anforderungen des Art. 30 Abs. 2 DS-GVO genügt. Hinsichtlich des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers hat der Auftragnehmer den Auftraggeber auf Anforderung in dem ihm möglichen Umfang zu unterstützen.

(10) Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung zu stellen. Er erteilt auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.

(11) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind.

§ 3. Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der jeweils einschlägigen Datenschutzgesetze sowie die Wahrung der Betroffenenrechte verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber geltend zu machen.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 4. Rechte des Auftraggebers / Kontrollen

(1) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der Datenverarbeitung zu erteilen. Gleiches gilt für die Festlegung bzw. Fortschreibung der Datensicherungsmaßnahmen. Sofern diese Anweisungen die Pflichten des Auftragnehmers wesentlich ändern oder zusätzliche Kosten verursachen, gelten sie als Antrag auf Änderung des Hauptvertrags.

(2) Der Auftraggeber oder ein Beauftragter des Auftraggebers kann sich nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen. Der Auftragnehmer hat die entsprechenden Kontrollen zu dulden und wird den Auftraggeber bei deren Durchführung unterstützen. Der Prüfer unterzeichnet auf Verlangen des Auftragnehmers vor der Kontrolle eine Vertraulichkeitsvereinbarung.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Kontrolle vernünftigerweise erforderlich sind.

(4) Soweit auf Seiten des Auftragnehmers bei der Unterstützung für Kontrollen Kosten entstehen, hat der Auftraggeber diese Kosten auf Grundlage der üblichen Tages-/Stundensätze des Auftragnehmers zu ersetzen, es sei denn, die Kontrollen sind aufgrund eines vom Auftragnehmer zu vertretenden Verstoßes gegen diese Vereinbarung oder gegen geltendes Gesetz nötig geworden, oder durch die Kontrolle werden Verstöße des Auftragnehmers gegen diese Vereinbarung oder geltendes Gesetz aufgedeckt.

§ 5. Subunternehmer

(1) Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit schriftlicher Genehmigung des Auftraggebers vergeben werden. Dies und die nachfolgenden Regelungen gelten auch für den Subunternehmer.

(2) Der Auftragnehmer hat den Auftraggeber über jede beabsichtigte Änderung in Bezug auf neue Subunternehmer zu informieren. Gegen solche Änderungen steht dem Auftraggeber ein Widerspruchsrecht zu.

(3) Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen. Er hat sich vor Beginn der Verarbeitung personenbezogener Daten durch den Subunternehmer und sodann regelmäßig von der Einhaltung der beim Subunternehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und die Ergebnisse zu dokumentieren. Dem Auftraggeber ist auf Verlangen der Prüfdokumentation zur Verfügung zu stellen.

(4) Die Auftragsvergabe an Subunternehmer muss mittels eines schriftlichen Vertrages erfolgen. Die vertraglichen Vereinbarungen sind so zu gestalten, dass sie den Anforderungen dieser Vereinbarung entsprechen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so umgesetzt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO und dieser Vereinbarung erfolgt.

(5) Der Auftraggeber ist berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(6) Sofern der Subunternehmer außerhalb eines in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stammt oder die Datenverarbeitung dort stattfindet, ist durch den Auftragnehmer darüber hinaus sicherzustellen, dass die Voraussetzungen der Art. 44 bis 49 DS-GVO erfüllt sind. Dies ist dem Auftraggeber gegenüber schriftlich vor Aufnahme der Tätigkeiten des Subunternehmers nachzuweisen.

(7) Die Genehmigung zur Einschaltung der Dienstleister in Anlage 5 gilt als erteilt, sofern die vorstehenden Anforderungen erfüllt sind.

(8) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten eines jeden Subunternehmers.

§ 6. Vertraulichkeit

(1) Die Parteien verpflichten sich, die ihnen während der Durchführung dieses Vertrages zur Kenntnis gelangten Informationen und Unterlagen, insbesondere Geschäfts- und Betriebsgeheimnisse des Vertragspartners streng vertraulich zu behandeln. Ebenso vertraulich zu behandeln sind der Gegenstand und Inhalt des Vertrages. Die Parteien sind verpflichtet, die zur Verfügung gestellten oder im Rahmen des Auftrages zur Kenntnis genommenen Daten und Informationen des Vertragspartners ausschließlich im Rahmen des Vertragszwecks zu verarbeiten und zu nutzen. Eine Verarbeitung oder Nutzung für eigene Zwecke sowie eine Weitergabe an Dritte ist nur nach schriftlicher Zustimmung des Vertragspartners zulässig, es sei denn, es handelt sich bei dem Dritten um einen (Rechts-)Berater der Vertragspartei mit beruflicher Schweigepflicht.

(2) Sofern zur Abwicklung des Auftrages die Einschaltung Dritter erforderlich ist, wird dafür Sorge getragen, dass die getroffenen Datenschutz- und Geheimhaltungsvereinbarungen von diesen Dritten ebenfalls strikt eingehalten werden. Die Einschaltung von Dritten erfordert das ausdrückliche Einverständnis des Vertragspartners.

(3) Die vorstehenden Rechte und Pflichten gelten über die Dauer dieser Vereinbarung und des Hauptvertrags fort.

§ 7. Beendigung des Vertrages

(1) Nach Beendigung des Vertrages oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinem Besitz befindlichen Unterlagen, Datenträger oder sonstigen Ergebnisse auf Wunsch des Auftraggebers physisch zu löschen bzw. diesem restlos mit der Erklärung zurückgeben, dass sich keine weiteren Kopien beim Auftragnehmer oder bei Unterauftragnehmern befinden. Beim Auftragnehmer gespeicherte Daten sind physisch zu löschen, mit Ausnahme von eingeschränkten personenbezogenen Daten in Back-ups, die nach den regulären Löschungsfristen gelöscht werden. Die Löschung ist zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten bzw. zu löschen.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(3) Der Auftraggeber ist berechtigt, die Einhaltung der vorstehenden Verpflichtungen, ggf. auch vor Ort, gemäß § 4 zu kontrollieren.

§ 8. Sonstiges, Allgemeines

(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 an den Daten beim Auftraggeber liegt.

(2) Diese Vereinbarung ersetzt alle zuvor getroffenen Vereinbarungen zum Datenschutz zwischen dem Auftraggeber und dem Auftragnehmer.

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung 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.

(4) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden oder der Vertrag eine Lücke enthalten, so bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Anstelle der unwirksamen oder fehlenden Bestimmung gilt eine wirksame Bestimmung als vereinbart, die dem von den Parteien Gewollten wirtschaftlich am nächsten kommt.

(5) Es gilt deutsches Recht.

Anlage 1: Leistungsbeschreibung

Die Tätigkeiten des Auftragnehmers für den Auftraggeber im Rahmen der Verarbeitung personenbezogener Daten des Verantwortlichen sind der Leistungsbeschreibung der jeweils beauftragten und vertraglich im Hauptvertrag zwischen den Parteien festgelegten Leistungen zu entnehmen.

Soweit die Leistungen A1007, D1001, A1044, A1045, A1128, A1134, A1140, A1066, SBC0003, A1113, D1008, D1009, D1011, D1013, D1014, D1015, D1016, D1017, D1018, D1019, D1010, D1006 beauftragt wurden, umfasst die Verarbeitungstätigkeit auch das Hosting personenbezogener Daten.

Keine für das Auftragsverarbeitungsverhältnis relevanten Verarbeitungen personenbezogener Daten enthalten die folgenden in der Leistungsbeschreibung aufgeführten Produkte des Auftragnehmers:

D1007, SBC0001, SBC0002, A1008, A1054, A1017, A1018, A1019, A1020, A1021, A1022, A1024, A1030, A1038, A1039, A1043, A1050, A1059, A1061, A1063, A1064, A1065, A1070, A1079, A1080, A1081, A1082, A1083, A1085, A1086, A1087, A1088, A1089, A1090, A1092, A1093, A1094, A1095, A1097, A1098, A1099, A1103, A1111, A1112, A1114, A1115, A1119, A1120, A1121, A1122, A1123, A1124, A1126, A1127, A1129, A1130, A1131, A1132, A1133, A1135, A1136, A1137, A1138, A1139, A1141, A1142, A1143, A1001, A1002, A1029, A1048, A1053, A1067, A1102, A1106, A1037, A1046, A1047, A1068, A1091, A1071, A1072, A1073, A1074, A1075, A1084, A1049, A1051, A1052, A1069, A1107, A1108, A1109, A1110, A1116

Anlage 2: Betroffene und Datenkategorien

Der Auftragnehmer verarbeitet vertragsgemäß auch personenbezogene Daten für den Auftraggeber. Diese werden im Folgenden spezifiziert. Bedingt durch den technologischen Wandel und organisatorischen Veränderungen kann sich die Zusammensetzung der Daten auch verändern.

Betroffene Personen sind insbesondere:

- Aktuelle und ehemalige Beschäftigte des Auftraggebers;
- Bewerber des Auftraggebers;
- Geschäfts- und Privatkunden des Auftraggebers (inklusive Interessenten) und Mitarbeiter von Geschäftskunden des Auftraggebers,
- Lieferanten des Auftraggebers und Mitarbeiter von Lieferanten des Auftraggebers,
- Sonstige Geschäftspartner des Auftraggebers und Mitarbeiter von sonstigen Geschäftspartnern des Auftraggebers.

Betroffene Kategorien personenbezogener Daten sind insbesondere:

- Stamm- und Kommunikationsdaten (u.a. Name, Geburtsname, Anrede, Titel, Geschlecht, Geburtsdatum, Familienstand, Nationalität, Sprache)
- Identitätsdaten (u.a. Personalnummer)
- Private und Berufliche Kontaktdaten (u.a. Anschrift, E-Mail-Adresse, Telefonnummer, Mobilnummer)
- Bewerbungsunterlagen (Qualifikationen, Ausbildung, Referenzen etc.)
- Reiseantragsdaten (u.a. Reisetätigkeit, Reisekosten, Reiseziel, Reisegrund, Reisespesen)
- Daten von BDE-Systemen (Betriebsdatenerfassung)
- Organisatorische Zuordnung von Beschäftigten (u.a. Abteilungszugehörigkeit, Kostenstelle, Tätigkeitsbeschreibung, Mitarbeitergruppe, Position im Unternehmen)
- Lohn- und Gehaltsdaten sowie Kreditkartendaten
- Zeiterfassungsdaten
- Daten der Mitarbeiter in CRM-Systemen (Vertrieb, Service-Center)
- Incident-Management-/Ticket-Systeme
- IT-System-spezifische Daten, wie z. B. User-Name, Zugriffsrechte, Nutzerprofile

Es findet keine Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DS-GVO statt.

Anlage 3: Technische und organisatorische Schutzmaßnahmen

1. Zutrittskontrolle

Die Zutrittskontrolle umfasst alle Maßnahmen, die gewährleisten, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Zutrittskontrolle stellt sicher, dass nur befugte Personen Zutritt zu den für sie freigegebenen Bereichen erhalten. Zu diesen Bereichen zählen u.a. Räume, Gebäude, Freigelände-Areale oder auch Stockwerke. Zutrittsberechtigungen können individuell oder für bestimmte Personengruppen gewährt werden, wobei auch zeitliche Befristungen definiert werden können. Es gibt verschiedene Arten eine Zutrittskontrolle durchzuführen. Dazu zählen personengestützte und rein elektronische Verfahren.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☒ Schlüsselregelungen / Konzept
☒ Automatische Zugangskontrolle	☒ Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☒ Besucherbuch / Protokoll der Besucher
☒ Chipkarten / Transpondersysteme	☒ Mitarbeiter - / Besucherausweise
☐ Manuelles Schließsystem	☒ Besucher in Begleitung durch Mitarbeiter
☒ Sicherheitsschlösser	☒ Sorgfalt bei der Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☒ Sorgfalt bei der Auswahl Reinigungsdienste
☒ Absicherung der Gebäudeschächte	☐
☒ Türen mit Knauf Außenseite	☐
☒ Klingelanlage mit Kamera	☐
☐ Videoüberwachung der Eingänge	☐
☒ Maßnahmen gegen Auswirkungen von Naturkatastrophen, vorsätzlichen Angriffen oder Unfällen	☐

2. Zugangskontrolle

Die Zugangskontrolle umfasst alle Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
Mit Hilfe der Zugangskontrolle wird die unbefugte Nutzung von IT-Systemen unterbunden. Eine zentrale Rolle nimmt die Identifikation von Usern oder Rechnern und ihre anschließende Authentifikation ein. Die Zugangskontrolle muss zudem die Zugangsdaten vor Missbrauch schützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzernamen + Passwort	☒ Verwalten von Benutzerberechtigungen
☐ Login mit biometrischen Daten	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software Clients	☒ Richtlinie „Sicheres Passwort“
☐ Anti-Virus-Software mobile Geräte	☒ Richtlinie „Löschen / Vernichten“
☒ Firewall	☒ Richtlinie „Clean desk“
☒ Intrusion Detection System	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☐ Mobile Device Management	☒ Mobile Device Policy
☒ Verschlüsselung von Datenträgern	☒ Anleitung „Manuelle Desktopsperre“
☒ Verschlüsselung Smartphones	☐
☐ Gehäuseverrieglung	☐
☐ BIOS Schutz (separates Passwort)	☐
☒ Sperre externer Schnittstellen (USB)	☐
☒ Automatische Desktopsperre	☐
☒ Verschlüsselung Laptop/Tablet	☐

3. Zugriffskontrolle

Die Zugriffskontrolle umfasst alle Maßnahmen um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Zugriffskontrolle ist die Überwachung und Steuerung des Zugriffs auf bestimmte Ressourcen. Das Ziel der Zugriffskontrolle ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten Es gibt zwei hauptsächliche Arten von Maßnahmen zur Zugriffskontrolle: physische und logische.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Externer Aktenvernichter (DIN 32757)	☒ Minimale Anzahl von Administratoren
☐ Physische Löschung von Datenträgern	☒ Datentresor
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung der Daten	☒ Verwaltung der Benutzerrechte durch Administratoren
☒ Regeln zur Verschlüsselung zum Schutz von Informationen bei Speicherung und Transport	☒ Richtlinie „Löschen / Vernichten“

4. Trennungskontrolle

Die Trennungskontrolle umfasst alle Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Durch geeignete Maßnahmen muss verhindert werden, dass die Daten gemischt werden können. Hauptanwendungsfälle der Trennungskontrolle sind etwa die Mandantenfähigkeit, Rollenkonzepte bei Anwendungen oder die Trennung von Systemen für Entwicklung, Test und Produktion.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☐ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankenrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☐ Datensätze sind mit Zweckattributen versehen

5. Pseudonymisierung

Die Pseudonymisierung ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Im Gegensatz zur Anonymisierung bleiben bei der Pseudonymisierung Bezüge verschiedener Datensätze, die auf dieselbe Art pseudonymisiert wurden, erhalten. Die Pseudonymisierung ermöglicht also – unter Zuhilfenahme eines Schlüssels – die Zuordnung von Daten zu einer Person, was ohne diesen Schlüssel nicht oder nur schwer möglich ist, da Daten und Identifikationsmerkmale getrennt sind. Entscheidend ist also, dass eine Zusammenführung von Person und Daten noch möglich ist.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Im Fall der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten Systemen (mögl. verschlüsselt)	☐ Interne Anweisung, Informationen im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

6. Weitergabekontrolle

Die Weitergabekontrolle umfasst alle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Durch die Weitergabekontrolle sollen die Integrität und die Vertraulichkeit während der Weitergabe gewährleistet sein. Des Weiteren soll der Empfänger der Daten ausreichend geprüft und festgestellt werden. Dabei umfasst die Weitergabekontrolle jede Art von Übermittlung, auch eine Datenverarbeitung innerhalb der verantwortlichen Stelle oder an einen Auftragsverarbeiter. Die Weitergabekontrolle bestimmt zulässige Empfänger der Daten und Übertragungswege.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ E-Mail Verschlüsselung	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Einsatz von VPN	☐ Übersicht regelmäßiger Abruf-und Übermittlungsvorgänge
☐ Protokollierung der Zugriffe und Abrufe	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☒ Sorgfalt bei der Auswahl von Transportpersonal und Fahrzeugen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftps, https	☐ Persönliche Übergabe mit Protokoll
☐ Datenübertragung per OFTP2	☐
☐ Nutzung von Signaturverfahren	☐

7. Eingabekontrolle

Die Eingabekontrolle umfasst alle Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Da die Daten letztlich zu Revisions- und Beweiszwecken verwendet werden, müssen die Daten vollständig sein, dürfen nur den berechtigten Personen zugänglich sein und nicht nachträglich verändert werden können. Zur Umsetzung der Eingabekontrolle ist die verantwortliche Stelle angehalten, die Erhebung, Verarbeitung und Nutzung von Daten umfassend zu protokollieren.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuellen Benutzernamen (nicht Benutzergruppen)
☐	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	☐ Aufbewahrung von Formularen, von denen Daten in automatisierter Verarbeitung übernommen wurden
☐	☐ klare Zuständigkeit von Löschungen

8. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle umfasst alle Maßnahmen um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Verfügbarkeitskontrolle ist damit ein Kernelement der IT-Sicherheit. Dabei geht es nicht nur um den Schutz vor "zufälligen" Ereignissen, sondern vielmehr um die Absicherung gegen sämtliche nicht außerhalb jeder Wahrscheinlichkeit liegenden Störungen und Schäden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlage	☒ Back-Up & Recovery Konzept
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraum klimatisiert	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ USV (unterbrechungsfreie Stromversorgung)	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ Schutzsteckdosenleisten Serverraum	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐ Datentresor	☐ Existenz eines Notfallplans
☒ RAID System / Festplattenspiegelung	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ Videoüberwachung Serverraum	☐
☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐
☒ Einsatz von VMware Hochverfügbarkeitslösung	☐
☒ Einsatz Veeam Backup & Replication Technologie	☐
☒ Proactive Care für Storage Systeme	☐

9. Datenschutzmanagement

Datenschutzmanagement ist eine Methode, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren. Ein systematisches Datenschutzmanagement ist wichtig, um im Fall von aufsichtbehördlichen Verfahren, den Vorwurf des fahrlässigen Handelns abschwächen zu können.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösung für Datenschutz-Management im Einsatz	☒ Externer Datenschutzbeauftragter Dr. Jörn Voßbein / UIMC Dr. Voßbein GmbH & Co KG / datenschutz.rocon@uimc.de 0202 9467726200
☒ zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (via Wiki; Intranet …)	☒ Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☒ Regelmäßige Sensibilisierung der Mitarbeiter (jährlich)
☒ Anderweitiges dokumentiertes Sicherheitskonzept	☐ Interner / externer Informationssicherheitsbeauftragter Name / Firma / Kontaktdaten
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird min. jährlich durchgeführt	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
☐	☒ Die Organisation kommt den Informationspflichten nach Artikel 13 und 14 DSGVO nach
☐	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐	☒ Vor dem Austausch von Informationen werden Geheimhaltungsvereinbarungen abgeschlossen, die Anforderungen bzw. Erfordernisse zum Schutz der Informationen werden dokumentiert und regelmäßig überprüft

10. Incident-Response-Management

Unter Incident Response (Vorfallreaktion) versteht man die Reaktion eines Unternehmens auf einen IT-Sicherheitsvorfall. Dazu zählen alle organisatorischen und technischen Maßnahmen zur Abwehr und schnellen Eindämmung des Vorfalles, damit der Schaden möglichst gering bleibt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch in Hinblick auf Meldepflicht an Behörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von DSB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Intrusion Prevention System (IPS)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☒ Informationen über technische Schwachstellen der IT-Systeme werden zeitnah beschafft, beurteilt und geeignete Maßnahmen ergriffen	☐

11. Datenschutzfreundliche Voreinstellungen

Datenschutzfreundliche Vorstellungen (Privacy by Default) bedeutet, dass bereits die Werkeinstellungen datenschutzfreundlich auszugestalten sind, um nicht dem Nutzer die Verantwortung für die entsprechenden Einstellungen zu übertragen.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Es werden nicht mehr Daten erhoben, als für den jeweiligen Zweck erforderlich ist	☐
☐ Einfache Umsetzung des Widerrufs eines Betroffenen durch technische Maßnahmen	☐

12. Auftragskontrolle (im Falle des Einsatzes von Subunternehmern)

Die Auftragskontrolle umfasst alle Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Auftragskontrolle soll sicherstellen, dass die verantwortliche Stelle „Herr der Daten“ bleibt, auch wenn Dienstleister im Rahmen ihrer delegierten Aufgaben mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Sorgfältige Auswahl des Auftragnehmers
	☒ Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
	☒ Schriftliche Weisung an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Informationsgeheimnis
	☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer
	☐ Verpflichtung zur Bestellung eines Informationssicherheitsbeauftragten durch den Auftragnehmer
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Sicherstellung der Vernichtung von Informationen nach Beendigung des Auftrags
	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und dessen Schutzniveau
	☒ Vor dem Austausch von Informationen werden Geheimhaltungsvereinbarungen abgeschlossen, die Anforderung bzw. Erfordernisse zum Schutz der Informationen werden dokumentiert und regelmäßig überprüft

Anlage 4: Betriebliche Datenschutzbeauftragte

Datenschutzbeauftragter des Auftragnehmers:

Name:	Dr. Jörn Voßbein (UIMC Dr. Voßbein GmbH & Co KG)
Anschrift:	Nützenberger Straße 119, 42115 Wuppertal
Telefonnummer:	(0202) 265 74 - 0

Anlage 5: Unterauftragnehmer gemäß § 5 des Vertrags

Dienstleister 1:

Name des Dienstleisters:	NetPlans IT-Systeme GmbH
Anschrift:	Bingener Strasse 21a, 55469 Simmern
Art der Dienstleistung:	Rechenzentrumsdienstleistungen
Bestellter Datenschutzbeauftragter (DSB):	NetPlans GmbH, Herr Murat Peker
Kontaktdaten des DSB:	Eisenstockstraße 12, D-76275 Ettlingen

Dienstleister 2:

Name des Dienstleisters:	TelemaxX Telekommunikation GmbH
Anschrift:	Postfach 41 09 27, 762009 Karlsruhe
Art der Dienstleistung:	Rechenzentrumbetrieb
Bestellter Datenschutzbeauftragter (DSB):	Thomas Steinle, LL.M. (legal informatics)
Kontaktdaten des DSB:	xDSB Datenschutz, Greschbachstrasse 6a, 76229 Karlsruhe/ Germany