Auftragsdatenvereinbarung gemäß Art. 28 Datenschutzgrundverordnung (DS-GVO)

nachstehend Auftrag/Vereinbarung genannt

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt –

ggf.: Vertreter gemäß Art. 27 DS-GVO:

nachfolgend einzeln oder gemeinsam: „Parteien“ genannt

PRÄMBEL

Die Parteien haben am einen Vertrag über die Erbringung von Leistungen im Zusammenhang mit personenbezogenen Daten geschlossen (nachfolgend: „Hauptvertrag“) genannt. Dieser Vertrag konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus dem Hauptvertrag ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer, Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1 GEGENSTAND, DAUER, ART, UMFANG UND ZWECK DER VERARBEITUNG (ART. 28 ABS. 3 S. 1 DS-GVO)

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers zur Erfüllung seiner vertraglichen Pflichten gegenüber dem Auftraggeber. Gegenstand, Zweck, Dauer, Art und Umfang der Verarbeitung einschließlich der Kategorien von Betroffenen ergeben sich aus Anlage 1.

2 PFLICHTEN UND RECHTE DES AUFTRAGGEBERS (ART. 28 ABS. 3 S. 1 DS-GVO)

Die Pflichten und Rechte des Auftraggebers gem. Art. 28 Abs. 3 S. 1 DS-GVO ergeben sich aus dem Hauptvertrag und diesem Vertrag.

3 VERPFLICHTUNG EINGESCHALTETER PERSONEN (ART. 28 ABS. 3 S. 2 LIT B DS-GVO)

Der Auftragnehmer verpflichtet zur Verarbeitung der personenbezogenen Daten eingesetzte oder befugte Personen vorab zur Vertraulichkeit und Wahrung des Datengeheimnisses oder stellt sicher, dass sie einer angemessenen gesetzlichen Verschwiegenheitspflicht in Bezug auf die personenbezogenen Daten unterliegen. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

4 TECHNISCH-ORGANISATORISCHE MASSNAHMEN (ART. 28 ABS. 3 S. 2 LIT C DS-GVO)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 2].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5 UNTERAUFTRAGSVERHÄLTNISSE

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. Er erlegt dem Unterauftragnehmer vorab vertraglich oder durch ein anderes anwendbares Rechtsinstrument nach dem Recht der Europäischen Union oder des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auf, die zwischen ihm und dem Auftraggeber in diesem Vertrag oder durch ein anderes anwendbares Rechtsinstrument des Rechts der Europäischen Union festgelegt sind.

(2) Der Auftraggeber stimmt der Beauftragung der in Anlage 1 aufgezählten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO. Der Einsatz von weiteren Unterauftragnehmern, die nicht in Anlage 1 genannt sind, bedarf zur Rechtmäßigkeit der vorherigen schriftlichen Genehmigung des Auftraggebers. Der Auftraggeber darf eine solche Genehmigung nicht missbräuchlich oder grundlos verweigern.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

6 ORT DER VERARBEITUNG

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, oder der Schweiz. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Der Auftraggeber erteilt hiermit seine ausdrückliche Zustimmung, dass die vertraglich vereinbarte Datenverarbeitung in die Schweiz verlagert und dort stattfinden kann.

7 UNTERSTÜTZUNG DES AUFTRAGGEBERS BEI DER ERFÜLLUNG DATENSCHUTZRECHTLICHER PFLICHTEN

(1) Der Auftragnehmer unterstützt den Auftraggeber nach seinen Möglichkeiten bei der Beantwortung von Anfragen betroffener Personen, der Information von betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten und der Umsetzung der Rechte der betroffenen Personen in Bezug auf die verarbeiteten Daten. Der Auftragnehmer beantwortet Auskunftsanfragen und andere Begehren (bspw. wie Ersuchen zur Löschung, Berichtigung oder Einschränkung personenbezogener Daten) von betroffenen Personen nicht selbst, sondern verweist die betroffenen Personen insoweit an den Auftraggeber.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Implementierung und Umsetzung technischer und organisatorischer Maßnahmen des Auftraggebers, der gesetzlich erforderlichen Meldung von Datenschutzverletzungen an die Datenschutzaufsichtsbehörden, bei der gesetzlich erforderlichen Benachrichtigung von betroffenen Personen über Datenschutzverletzungen, bei gesetzlich erforderlichen Pflichten zur Datenschutz-Folgenabschätzung und gesetzlich erforderlichen Abstimmungen mit der Datenschutzaufsichtsbehörde.

3) Für Unterstützungsleistungen, die nicht in dem Hauptvertrag enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

8 BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

9 LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

(1) Kopien oder Duplikate der Daten 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist unaufgefordert vorzulegen.

(3) 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.

10 DATENSCHUTZRECHTLICHE PFLICHTEN DES AUFTRAGNEHMERS, NACHWEIS DER EINHALTUNG UND KONTROLLRECHTE (ART. 28 ABS. 3 S. 2 LIT H, 31 DS-GVO)

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die getroffenen technischen und organisatorischen Maßnahmen um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(5) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

Der Auftragnehmer bestellt einen Datenschutzbeauftragten, soweit er gesetzlich dazu verpflichtet ist

Datenschutzbeauftragter des Auftragnehmers ist:

Herr

Kargl Rolf-Dieter

dsb@trivadis.com

(6) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(7) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 2].

(8) Der Auftragnehmer führt das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO und stellt dies dem Auftraggeber auf Anforderung zur Verfügung.

(9) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung seiner vertraglichen und gesetzlichen Pflichten als Auftragsverarbeiter zur Verfügung. Er gestattet und ermöglicht dem Auftraggeber und von ihm beauftragten Prüfern entsprechende Überprüfungen – einschließlich Inspektionen – und trägt in zweckmäßigem Maß dazu bei. Überprüfungen sind mindestens 30 Kalendertage im Voraus beim Auftragnehmer anzumelden.

(10) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

(11) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesem Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(12) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

11 VERARBEITUNG PERSONENBEZOGENER DATEN NUR AUF DOKUMENTIERTE WEISUNG (ART. 28 ABS. 3 S. 2 LIT. A DS-GVO)

(1) Der Auftragnehmer verarbeitet und übermittelt personenbezogene Daten des Auftraggebers nur auf dokumentierte Weisung des Auftraggebers. Das gilt insbesondere für die Übermittlung personenbezogener Daten des Auftraggebers an einen Empfänger in einem Drittland oder an eine internationale Organisation; diese darf nur mit ausdrücklicher Genehmigung des Auftraggebers erfolgen und nur, soweit die Voraussetzungen von Kapitel V der DS-GVO erfüllt sind. Der Auftraggeber erteilt hiermit seine ausdrückliche Einwilligung zur Übermittlung personenbezogener Daten in die Schweiz sowie deren dortigen Verarbeitung.

(2) Die Weisungen werden anfänglich durch diesen Vertrag und den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden.

(3) Der Auftragnehmer darf personenbezogene Daten des Auftraggebers auch verarbeiten und übermitteln, wenn er hierzu durch das Recht der Europäischen Union oder eines Mitgliedstaats verpflichtet ist. In diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

12 INFORMATION ÜBER DATENSCHUTZWIDRIGE WEISUNGEN, WEISUNGSBEFUGNIS DES AUFTRAGGEBERS (ART. 28 ABS. 3 S. 3. ART. 28 ABS. 3 S. 2 LIT. A DS-GVO)

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

13 MITTEILUNG BEI VERSTÖßEN DES AUFTRAGNEHMERS

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei unrechtmäßiger Kenntniserlangung der personenbezogenen Daten durch Dritte oder bei sonstigen schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder in diesem Vertrag getroffene Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Die vorstehende Mitteilungspflicht greift stets dann, wenn die Möglichkeit nicht ausgeschlossen werden kann, dass der Verstoß zu einer Meldepflicht des Auftraggebers nach Art. 33 Abs.1 DS-GVO oder Art. 34 Abs. 1 DS-GVO führt.

14 WEITERE PFLICHTEN UND SCHLUSSBESTIMMUNGEN

(1) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Datenschutzbeauftragter des Auftraggebers ist:

(2) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren, durch Verlangen nach Offenlegung im Zusammenhang mit gerichtlichen Verfahren 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 Verantwortlichem im datenschutzrechtlichen Sinne liegen.

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises, dass es sich um eine Änderung beziehungsweise Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Bei etwaigen Widersprüchen gehen die Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages vor.

Auftragnehmer	**Auftraggeber**
Unterschrift	**Unterschrift**

ANLAGE 1 – ANGABEN ZUR VERARBEITUNG

Gegenstand der Verarbeitung und Zweck

(Hinweis: Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)

Art der personenbezogenen Daten

Folgende personenbezogene Daten werden verarbeitet:

☐ Personenstammdaten

☐ Kontaktdaten (z.B. Telefon, E-Mail)

☐ Bewerbungsdaten (z.B. Lebenslauf, Zertifikat, u. U. Grad der Behinderung)

☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Kundenhistorie

☐ Vertragsabrechnungs- und Zahlungsdaten

☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

☐ Andere - Bitte beschreiben:

Kategorien der Betroffenen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Kunden

☐ Bewerber

☐ Interessenten

☐ Abonnenten

☐ Beschäftigte

☐ Lieferanten

☐ Handelsvertreter

☐ Ansprechpartner (z.B. Vermittler)

☐ Andere- Bitte beschreiben:

Dauer der Verarbeitung

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

☐ Dauer der Verarbeitung ist:

Unterauftragnehmer

Unterauftragnehmer (Firmenname)	Kontaktdaten	Ort der Verarbeitung	Beschreibung der Dienstleistung

Fachliche Ansprechperson

Fachliche Ansprechperson des Auftraggebers:

Fachliche Ansprechperson des Auftragnehmers:

ANLAGE 2 – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

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

Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;	• Kartengestützte personalisierte Zutrittskontrollsysteme mit Zutrittsberechtigung nur für autorisierte Mitarbeiter, • Dienstanweisungen zur Handhabung von Zutrittskontrollen, • Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude • Server in abschließbaren Serverschränken, Schlüssel bei IT-Abteilung, • Organisationsanweisung zur Ausgabe von Schlüsseln, • Verschluss von Laptops in Schränken nach Dienstschluss, • Abschließen des Gebäudes nach Arbeitsschluss sowie Sicherung durch Alarmanlage
Zugangskontrolle Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;	• Serversysteme nur mit Konsolenpasswort oder über passwortgeschützte, verschlüsselte Verbindung administrierbar • Datenverschlüsselung • Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar • Zeitliche Sperrung des Benutzerkontos nach fünf fehlgeschlagenen Anmeldeversuchen • Automatische, passwortgeschützte Bildschirm- und Rechnersperre nach 10 Minuten • Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine unpersönlichen Sammelkonten („AZUBI1“) • Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passwörter/Smartcards • Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner)
Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;	• Datenverschlüsselung • Trennung von Berechtigungsbewilligung (organisatorisch) durch Abteilungsleitung / Geschäftsleitung / Geschäftsführung und Berechtigungsvergabe (technisch) durch IT-Abteilung • Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(gruppen)

Trennungskontrolle Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;	• Die Daten des AUFTRAGGEBERs und anderer Mandanten werden soweit möglich von unterschiedlichen Mitarbeitern des Dienstleisters verarbeitet • Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung von Daten des AUFTRAGGEBERs von Daten anderer Mandanten Rechnung trägt • Die in den verwendeten Systemen verfügbaren Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzeptes

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

Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;	• Versand personenbezogener Daten, z.B. per verschlüsselter E-Mail • Datenverschlüsselung • Leitungsverschlüsselung
Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;	• Vertragliche Beschränkung der Arbeit mit personenbezogenen Daten des AUFTRAGGEBERs auf die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeiter des Dienstleisters

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

Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;	• Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophen-sicherer Aufbewahrung der Datenträger • Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes (Virenschutz-konzept usw.) • Einsatz unterbrechungsfreier Stromversorgung
Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.	• Der Vertrag enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des AUFTRAGGEBERs • Der Vertrag enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des AUFTRAGGEBERs sowie ein Verbot der Nutzung durch den Dienstleister ausserhalb des schriftlich formulierten Auftrags • Der Dienstleister hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die

	Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO); z. B. Durch: Backup-Konzept, Redundante Datenspeicherung, Doppelte IT-Infrastruktur, Schatten-Rechenzentrum	• Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophen-sicherer Aufbewahrung der Datenträger

ANLAGE 3 – STANDARDVERTRAGSKLAUSELN UND BESONDERE MAßNAHMEN BEIM DATENTRANSFER IN DRITTSTAATEN

(Hinweis: Kommen nur bei Datenübermittlung in Drittstaaten ohne Angemessenheitsbeschluss der EU zur Anwendung und müssen nicht gesondert ausgefüllt, oder unterzeichnet werden)

EU Standardvertragsklauseln (in der zum Vertragsabschluss gültigen Version)

CELEX_02010D0087-20161217_DE_TXT.pdf

Besondere Maßnahmen beim Datentransfer in Drittstaaten

(1) Erhält der Auftragnehmer ein rechtswirksames Ersuchen von Strafverfolgungsbehörden oder anderen Dritten, die die Offenlegung von personenbezogenen Daten, die dem für die Verarbeitung Verantwortlichen gehören, verlangen, ist der Auftragsverarbeiter verpflichtet, den Auftraggeber unverzüglich über ein solches Ersuchen zu benachrichtigen und die Strafverfolgungsbehörden oder Dritte anzuweisen, die Informationen direkt beim Auftraggeber und nicht beim Auftragnehmer einzuholen.

(2) Wenn es dem Auftragnehmer gesetzlich untersagt ist, den Auftraggeber zu benachrichtigen und die Strafverfolgungsbehörden oder Dritte weiterzuleiten, ist der Auftragnehmer verpflichtet, das gesetzliche Verbot anzufechten, um eine Weiterleitung oder Benachrichtigung des Auftraggeber zu ermöglichen. Bleibt eine solche Anfechtung erfolglos, ist es gemeinsames Verständnis der Parteien, dass der Auftragnehmer ein Verfahren anstrebt und falls möglich einleitet.

(3) Der Auftragnehmer wird keinem Dritten zur Verfügung stellen: (a) direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf personenbezogene Daten; (b) Plattform-Verschlüsselungsschlüssel, die zur Sicherung der verarbeiteten Daten verwendet werden, oder die Möglichkeit, diese Verschlüsselung zu brechen; oder (c) Zugriff auf personenbezogene Daten, wenn dem Auftragsverarbeiter bekannt ist, dass die Daten für andere als die im Antrag des Dritten angegebenen Zwecke verwendet werden sollen. Zur Unterstützung des Vorstehenden kann der Auftragnehmer dem Dritten die Kontaktinformationen des Auftraggeber zur Verfügung stellen.

(4) Die Parteien haben vereinbart, dass sie zusätzliche Vereinbarungen über zusätzliche Schutzmaßnahmen in Bezug auf die Übermittlung personenbezogener Daten in Drittländer, treffen werden, wenn dies von lokalen oder europäischen Datenschutzbehörden gefordert wird.