Auftragsverarbeitungsvereinbarung

Zwischen

a) Auftraggeber Wirtschaftsakteur – Unternehmen

Unternehmen	
Unternehmen	
Adresse	

–nachfolgend Auftraggeber genannt –

und

b) Auftragnehmer

Auftragnehmer
FMB Fischer Management Beratungs GmbH **FMB-Akademie / OVZ Verwaltungs GmbH**
Bretonischer Ring 6
85630 Grasbrunn

–nachfolgend Auftragnehmer genannt–

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO).
Auftraggeber und Auftragnehmer werden nachfolgend auch als „Vertragsparteien“ bezeichnet.

Präambel

(1) Der von beiden Vertragsparteien unterzeichnete Rahmenvertrag Akademie Partner zur Bereitstellung der Akademie Seminarmanagementsoftware wird nachfolgend als „Rahmenvertrag“ bezeichnet.

(2) Der Funktionsumfang der Cloudplattform ist im Rahmenvertrag festgelegt.

(3) Dieser Auftragsverarbeitungsvertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz nach Art. 28 DSGVO, die sich aus dem Rahmenvertrag ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit dem Rahmenvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Der Auftragnehmer stellt dem Auftraggeber eine Cloud-Plattform zur Organisation und Durchführung von Schulungen bereit.

1.1 Gegenstand des Auftrags sind folgende Dienstleistungen:

1. Bereitstellung der Cloudplattform
2. Ersteinrichtung von Benutzerkonten und Benutzerrollen
3. Erstellung von Formularen
4. Fehlerbehebungen
5. E-Mail-Support
6. Monitoring
7. Backup

1.2 Kategorien personenbezogener Daten

Folgende Kategorien personenbezogener Daten sind Gegenstand der Verarbeitungen

1. Browserinformationen und IP-Adressen
2. Nutzerdaten (Anmeldedaten und Nutzerrollen)
3. Informationen über Schulungsteilnehmer:
   Kontaktinformationen, Leistungs- und Qualifikationsinformationen, soweit sie vom Auftraggeber für Schulungen freigegeben wurden
4. Informationen über Trainer
   Kontaktinformationen, Leistungs- und Qualifikationsinformationen, soweit sie vom Auftraggeber für Schulungen freigegeben wurden
5. Kommunikationsdaten
6. Protokolldaten im Rahmen des Monitorings.

1.3 Kategorien Betroffener Personen

1. Mitarbeiter des Auftraggebers
2. Mitarbeiterdaten des Auftragnehmers
3. externe Trainer

Es werden vom Auftraggeber folgende personenbezogene Daten bereitgestellt und vom Auftraggeber erfasst, verarbeitet und gespeichert nach:

- **Kategorie 2**, Name, Digitale Identifikatoren-E-Mail-Account, Password
  Qualifikationsdaten, Qualitätsnachweise, Zertifikate
  Leistungsdaten Testergebnisse, Bewertungsergebnisse,
  Abrechnungsdaten

Der Auftraggeber trägt selbstständig Sorge für die ordnungsgemäße Einhaltung der rechtlichen Verpflichtung der DSGVO, insbesondere die firmeninternen Regelungen zu den personenbezogenen Daten seiner eingebuchten Mitarbeiter.

1.4 Laufzeit der Vereinbarung

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Rahmenvertrages.

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

(2) Der Auftraggeber kann den Rahmenvertrag i.V.m. dem Auftragsverarbeitungsvertrag jederzeit nach den Vorgaben des Rahmenvertrag und der FMB AGB's mit einer festgelegten einer Frist kündigen, wenn ein wichtiger Grund vorliegt, z.B. ein schwerwiegender Verstoß des Auftragnehmers gegen gesetzliche Datenschutzvorschriften oder die Bestimmungen dieses Vertrages, so insbesondere, wenn der Auftragnehmer eine Weisung des Auftraggebers schuldhaft nicht ausführen kann oder will oder der Auftragnehmer 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 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Rahmenvertrag und 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 DSGVO).

(2) Die Weisungen werden anfänglich durch den Rahmenvertrag 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) DSGVO 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 so lange 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 der DSGVO und des BDSG gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DSGVO) 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.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dessen Ersuch unverzüglich an den Auftraggeber weiterleiten.

(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 die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind 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. Externer Auftragnehmer verantwortliche Stelle ist FMB Fischer Management Beratungs GmbH / OVZ Verwaltungs GmbH, Alexander G.V. Fischer (a.fischer@fischer-management.de).

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO 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.

(9) Für die jeweils aktuellen ein und/oder ausgebuchten Daten der Mitarbeiter des Auftraggebers ist der Auftraggeber selbstständig verantwortlich.

(10) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
Hierzu gehört die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen 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.
Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(11) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers nach rechtlichen Vorgaben entweder herauszugeben oder zu löschen. Falls der Auftraggeber eine Aufbewahrung über das Vertragsende hinaus oder eine Datenweitergabe an Dritte wünscht, ist hierzu eine gesonderte Vereinbarung erforderlich.

§ 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 Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 9 Satz 3 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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 die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Daten-Portabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 6 Nachweismöglichkeiten

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

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei vom Auftraggeber gewünschte Kontrollen unterstützend mitwirkt.

(2) 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 Unterauftragsverhältnisse (weitere Auftragsverarbeiter)

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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

- Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer erfolgt nur nach Zustimmung des Auftraggebers in schriftlicher oder elektronischer Form.

- Der Auftraggeber erteilt hiermit seine Zustimmung zur Beauftragung der in der Anlage I aufgeführten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer.

- Der Auftragnehmer hat vertraglich sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des Auftragnehmers mit dem Subunternehmer muss schriftlich oder in elektronischem Format abgeschlossen werden.

- Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSDSGVO erfüllt sind.

- Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

- Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

- Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§8 Internationale Datentransfers

(1) 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. Ausgenommen hiervon sind die in Anlage 1 aufgeführten Dienste. In der Anlage 2 werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus entsprechend den Vorgaben aus Artt. 44 ff. DSGVO im Rahmen der Unterbeauftragung spezifiziert.
Eine weitere Verlagerung von Diensten an Unterauftragnehmer in ein Drittland bedarf der schriftlichen Zustimmung des Auftraggebers. Die Vorgaben aus Artt. 44 ff sind einzuhalten.

(2) Jede weitere Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung bzw. Zustimmung des Auftraggebers unter dem Vorbehalt der Erfüllung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

§ 9 Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend den in Art. 82 DSGVO getroffenen Regelungen.

(2) Im Verhältnis der Vertragsparteien untereinander finden die Haftungsregelungen des Vertrages entsprechende Anwendung auf diese Vereinbarung.

§ 10 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 Vereinbarung 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 Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Es gelten die aktuellen AGB‘s der FMB Fischer Management Beratungs GmbH; AVV-Auftragsverarbeitungsvertrages und FMB-Datenschutzrichtlinien. Diese sind dem Vertrag als Anlage beigefügt und wurden vom Auftraggeber zur Kenntnis genommen und anerkannt worden. Der Auftraggeber hat die Möglichkeit die rechtlich bindende AGB‘s, Datenschutzbestimmungen auf der Website www.fischer-management.de einzusehen.

Der Auftraggeber ist mit ihrer Geltung einverstanden. Durch Unterschrift der juristischen Person des Auftraggebers werden die Anlagen zu dem unterzeichneten Rahmenvertrag, sowie zu diesem AVV Vertrag bestätigt.

FMB Fischer Management Beratungs GmbH	**Kunde**
vertreten durch Geschäftsführer	vertreten durch den Geschäftsführer
Auftragnehmer	**Auftraggeber**
Grasbrunn,	Ort Datum
(Ort, Datum)	(Ort, Datum)
Unterschrift / Firmenstempel	Unterschrift / Firmenstempel

Anlage 1 – Subunternehmer

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistung	Angaben zu geeigneten Garantien
Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 United States	Hosting der Applikation im Rechenzentrum in Frankfurt am Main	Art. 46, Abs. 2 (Standard-Vertragsklauseln) mit ergänzenden Maßnahmen
NEXUAI PRIVATE LIMITED B601, 6th Floor, B wing, Mondeal Height SG Highway, Jodhpur Char Rasta, Ahmedabad Gujarat—380015, India Info: Tochterunternehmen der plus-IT GmbH	Programmierung Fehlerbehebung (bis auf Ausnahmen in Absprache mit Kunden kein Zugriff auf Kundendaten) Systemwartung (ohne Zugriff auf Kundendaten)	Art. 46, Abs. 2 (wie oben)
Matrixhive Solutions A501, 100ft Road Safal Pegasus, 100 Feet Anand Nagar Rd, Satellite, Ahmedabad, Gujarat 380015, India	Programmierung Fehlerbehebung (bis auf Ausnahmen in Absprache mit Kunden kein Zugriff auf Kundendaten) Systemwartung (ohne Zugriff auf Kundendaten)	Art. 46, Abs. 2 (wie oben)

Anlage 2 Technischen und organisatorischen Maßnahmen

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

Zutrittskontrolle

☒ Schlüssel / Schlüsselvergabe

☒ Zutrittsrechte für autorisierte Personen werden gemäß Sicherheitskriterien individuell erteilt. Dies gilt auch hinsichtlich externer Personen.

Zugangskontrolle

☒ Passwortverfahren

☒ Automatische Sperrmechanismen (z. B. Kennwort oder Pausenschaltung, Session-timeout, Bildschirmschoner)

☒ Regelmäßig aktualisierte Antiviren- und Spyware Filter im Netzwerk und auf den einzelnen PCs - Datenbank

☒ Verschlüsselung von Datenträgern

☒ Netzwerktrennung mit Firewall

☒ Zwei-Faktor-Authentifizierung

Zugriffskontrolle

☒ Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte

☒ Protokollierung von Zugriffen

☒ Regelmäßige Auswertung und Kontrolle bestehender Berechtigungen

☒ Zeitnahe Durchführung von Aktualisierung bzw. Löschung von Berechtigungen

☒ Protokollierung unberechtigter Zugriffe (System, Datenbanken) mit Alert

☒ Endpoint Security

☒ Härtung der Systeme nach anerkannten Standards (CIS-Benchmarks)

Trennungskontrolle

☒ Trennung von Test- und Produktivsystemen

☒ Rollenbezogenes Berechtigungskonzept

☒ Mandantenfähigkeit (logisch, auf Wunsch physisch)

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

Weitergabekontrolle

☒ Verschlüsselung (AES 256)

☒ Virtual Private Networks (VPN)

☒ Datenschutzgerechte Entsorgung von Datenträgern

Eingabekontrolle

☒ Zugriffe auf personenbezogene Daten erfolgen nur von autorisierten Benutzern auf der Grundlage eines rollenbezogenen Berechtigungskonzepts

☒ Eingabeprotokollierung

☒Dokumentenmanagement

Übertragungskontrolle

☒ Verschlüsselnde Übertragungsprotokolle

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

Verfügbarkeitskontrolle

- ☒ Redundante Datenverarbeitungssysteme
- ☒ Backup-Strategie, regelmäßige Datensicherung (online/offline; on-site/off-site)
- ☒ Regelmäßige Überprüfung der Wiederherstellbarkeit
- ☒ unterbrechungsfreie Stromversorgung (USV)
- ☒ Virenschutz
- ☒ Firewalls und andere Techniken der Netzwerksicherheit
- ☒ Meldewege und Notfallpläne; Business Continuity Management
- ☒ Zertifiziertes Rechenzentrum (ISO 27001; BSI C5:2020)

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

- ☒Backup-Strategie, regelmäßige Datensicherung und Überprüfung

Zuverlässigkeit

- ☒ Statusanzeigen zur Kontrolle der Systemverfügbarkeit und Stabilität
- ☒ Alerts bei unberechtigten Zugriffen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) Datenschutz-Management;

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

- ☒ Verschlüsselung

Nachweisbarkeit (Art. 5 Abs. 2 DS-GVO);

- ☒ Protokollierung der durchgeführten Maßnahmen
- ☒ Regelmäßige interne Pen-Tests
- ☒ Regelmäßige Code Reviews
- ☒ Jährliche Audits

Auftragskontrolle

- ☒ Eindeutige Vertragsgestaltung
- ☒ formalisiertes Auftragsmanagement
- ☒ strenge Auswahl des Dienstleisters
- ☒ Vorabüberzeugungspflicht
- ☒ Nachkontrollen