Auftragsverarbeitungsvertrag

Version 2

Stand 06.05.2026

zwischen

demjenigen Verantwortlichen, der diesem Auftragsverarbeitungsvertrag durch digitale Zustimmung vor Inanspruchnahme der Leistungen zugestimmt hat.

– nachfolgend bezeichnet als „**Verantwortlicher**" –

und

AiphaOmega UG (haftungsbeschränkt),
Reherweg 58, 31787 Hameln, Deutschland

als Auftragsverarbeiter (nachfolgend „**Auftragsverarbeiter**",
Verantwortlicher und Auftragsverarbeiter gemeinsam die „**Parteien**")

wird der folgende **Auftragsverarbeitungsvertrag** geschlossen:

*Alle Begrifflichkeiten verstehen sich **geschlechtsneutral**.*

Präambel

Der Verantwortliche hat den Auftragsverarbeiter im Vertrag (nachfolgend „Hauptvertrag") zu den dort genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (nachfolgend die „Vereinbarung"), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) **Verantwortlicher** ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) **Auftragsverarbeiter** ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) **Personenbezogene Daten** sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „Betroffener") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) **Besonders schutzbedürftige personenbezogene Daten** sind personenbezogene Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrische Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) **Verarbeitung** ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung,

Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) **Unterauftragsverarbeiter** bezeichnet einen weiteren Auftragsverarbeiter, dessen Dienste der Auftragsverarbeiter in Anspruch nimmt, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen.

(7) **Aufsichtsbehörde** ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

(8) **Hauptvertrag** bezeichnet jede zwischen den Parteien bestehende oder künftig geschlossene Vereinbarung, in deren Rahmen der Auftragsverarbeiter Leistungen erbringt, bei denen personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet werden. Der Begriff umfasst auch laufende oder künftige Einzelaufträge, Zusatzleistungen oder Erweiterungen, die im Rahmen der bestehenden Geschäftsbeziehung erbracht werden.

§ 2 Vertragsgegenstand

(1) Die Auftragsverarbeitung erfolgt im Rahmen des Hauptvertrages.

Gegenstand der Verarbeitung ist der Betrieb und die Bereitstellung der Plattform „**Regulint**" zu Schulungs- und Dokumentationszwecken durch die AiphaOmega UG (haftungsbeschränkt), einschließlich der Verwaltung von Nutzer- und Vertragsdaten sowie aller damit verbundenen technischen und organisatorischen Leistungen.

(2) Der Auftragsverarbeiter erbringt für den Verantwortlichen die im Hauptvertrag genannten Leistungen. Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, die der Auftragsverarbeiter für den Verantwortlichen ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag und etwaigen zugehörigen Leistungsbeschreibungen. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(3) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

(5) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind vom Verantwortlichen zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Arten der verarbeiteten Daten, Kreis der Betroffenen, Drittland

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf folgende Arten und Kategorien von personenbezogenen Daten.

- Name, Vorname, Anrede
- Mitarbeiter- / Personaldaten
- Kontaktdaten
- Vertragsdaten
- Kommunikations- / Verbindungsdaten
- Logfiles
- Firmendaten,
- Bank-, Finanz-, Konto-, Transaktionsdaten

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist:

- Mitarbeitende

- Kunden / Interessenten
- Webseitenbesucher
- Abonnenten

(3) Eine Weitergabe personenbezogener Daten in ein Drittland (außerhalb des EWR) darf unter den Voraussetzungen der Art. 44 ff. DSGVO stattfinden.

§ 5 Schutzmaßnahmen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in Anlage 2 genannten technischen und organisatorischen Maßnahmen (TOMs) zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Die TOMs dürfen entsprechend dem technischen und rechtlichen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Verantwortlichen mitgeteilt werden.

(3) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend “Mitarbeiter”), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

(4) Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte des Auftragsverarbeiters ist die exkulpa gmbh, Waldfeuchter Str. 266, 52525 Heinsberg, https://exkulpa.de/. Als externe Datenschutzbeauftragte ist Aurea Kindshofer, +492452993314, a.kindshofer@exkulpa.de benannt.

§ 6 Informationspflichten des Auftragsverarbeiters

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

(2) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

(3) Der Auftragsverarbeiter ist darüber hinaus verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragsverarbeiter den Verantwortlichen zu unterrichten.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche kann sich vor der Aufnahme der Datenverarbeitung und sodann jährlich, mit einer angemessenen Vorlaufzeit, die beim Auftragsverarbeiter bzw. dessen Unterauftragsverarbeiter anzumelden ist, von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern

dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

(2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

(3) Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsverarbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Unterauftragsverhältnisse und Einsatz von Dienstleistern

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 1 genannten Dienstleister (nachfolgend “Unterauftragsverarbeiter”) durchgeführt. Der Verantwortliche erteilt dem Auftragsverarbeiter seine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 S. 1 DSGVO, im Rahmen seiner vertraglichen Verpflichtungen weitere Unterauftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen.

(2) Der Auftragsverarbeiter wird den Verantwortlichen vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichen Grund Einspruch erheben.

(3) Der Einspruch gegen die beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters ist innerhalb von zwei (2) Wochen nach Erhalt der Information über die Änderung zu erheben. Wird kein Einspruch erhoben, gilt die Hinzuziehung oder Ersetzung als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen dem Verantwortlichen und dem Auftragsverarbeiter nicht möglich, steht dem Auftragsverarbeiter ein Sonderkündigungsrecht zum auf den Einspruch folgenden Monatsende zu.

(4) Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.

(5) Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu den Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

§ 9 Anfragen und Rechte Betroffener

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen an den Verantwortlichen und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragsverarbeiter allein der Verantwortliche gegenüber dem Betroffenen verantwortlich.

(2) Der Auftragsverarbeiter haftet für Schäden unbeschränkt, soweit die Schadensursache auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Auftragsverarbeiters, seines gesetzlichen Vertreters oder Erfüllungsgehilfen beruht.

(3) Für fahrlässiges Verhalten haftet der Auftragsverarbeiter nur bei Verletzung einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Verantwortliche regelmäßig vertraut und vertrauen darf, jedoch beschränkt auf den vertragstypischen Durchschnittsschaden. Im Übrigen ist die Haftung des Auftragsverarbeiters – auch für seine Erfüllungs- und Verrichtungsgehilfen – ausgeschlossen.

(4) Die Haftungsbegrenzung gemäß § 10 Abs. 3 gilt nicht für Schadensersatzansprüche aus der Verletzung von Leben, Körper, Gesundheit oder aus der Übernahme einer Garantie.

§ 11 Beendigung des Hauptvertrags

(1) Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung auf Anfrage zu führen.

(2) Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe oder Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu kontrollieren.

(3) Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

(4) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragsverarbeiter i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

§ 12 Schlussbestimmungen

(1) Soweit der Auftragsverarbeiter Unterstützungshandlungen nach dieser Vereinbarung nicht ausdrücklich kostenlos durchführt, kann er dem Verantwortlichen dafür eine angemessene Gebühr in Rechnung stellen, es sei denn, eigene Handlungen oder Unterlassungen des Auftragsverarbeiters haben diese Unterstützung unmittelbar erforderlich gemacht.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Das anwendbare Recht bestimmt sich nach dem Hauptvertrag.

(5) Der Gerichtsstand bestimmt sich nach dem Hauptvertrag.

Anlagen

Anlage 1 – Aktuelle Unterauftragsverarbeiter

Name	Adresse und Website	Funktion	Serverstandort
Postmark	https://postmarkapp.com 1 N Dearborn Street, Suite 500, Chicago, IL 60602, USA	E-Mail-Provider	EU
Render	https://render.com 525 Brannan St, Suite 300, San Francisco, CA 94107, USA	Back- & Frontend-Hosting	DE
Scaleway	https://www.scaleway.com 8 rue de la Ville l'Evêque, 75008 Paris, France	File Storage	EU
Strato	https://www.strato.de Otto-Ostrowski-Straße 7, 10249 Berlin, Germany	Website-Hosting & Domain	DE
Stripe	https://stripe.com One Wilton Park Wilton Place Dublin 2 D02 FX04 Ireland	Zahlungsdienst	EU
Supabase	https://supabase.com 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513	Datenbank	DE

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters (TOMs)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1. Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Manuelles Schließsystem (z. B. Schlüssel)
- Arbeit im Home-Office: Anweisung an Mitarbeiter, wenn möglich, in von Wohnräumen abgetrennten Arbeitszimmern zu arbeiten

1.2. Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Authentifikation mit Benutzer und Passwort im Administrations-Dashboard; Passwort-Hashing nach aktuellem Stand der Technik (OWASP-Empfehlung)
- Passwortlose Authentifizierung der Kursteilnehmer mittels kryptographisch signierter Einmal-Links
- Zeitlich begrenzte Session-Tokens mit automatischem Ablauf und serverseitigem Session-Tracking; regelmäßige Revalidierung der Sitzungsgültigkeit
- Rate-Limiting für Authentifizierungsanfragen mit nutzerfreundlichen Schwellenwerten
- Automatische Session-Invalidierung bei Passwortänderung
- Erstellen von Benutzerprofilen mit rollenbasierter Zuordnung und Berechtigung
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Verschlüsselung von mobilen Endgeräten (Smartphones, Notebooks, Tablets)
- Automatische Desktopsperre

1.3. Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Verwaltung der Benutzerrechte durch Systemadministratoren

- Anzahl der Administratoren ist auf das betrieblich notwendige Minimum beschränkt
- Rollenbasierte Zugriffskontrolle mit strikter Rollentrennung und abgestuften Berechtigungen für Kursteilnehmer, Unternehmens-, Mandanten-, Partner- und Plattform-Administratoren
- Serverseitige Validierung des Nutzerkontexts bei jeder API-Anfrage
- Hierarchisches Berechtigungsmodell: Nur primäre Administratoren können weitere Admins anlegen; Plattform-Administration ausschließlich für berechtigte Mitarbeiter des Auftragnehmers
- Automatische Session-Invalidierung bei unberechtigtem Zugriff
- Clientseitige Datenisolation: automatisches Löschen aller lokalen Sitzungsdaten bei Benutzer- oder Kurswechsel

1.4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (Multi-Tenancy) auf Datenbankebene: alle Datensätze sind einem Mandanten zugeordnet; technische Constraints verhindern mandantenübergreifende Zugriffe. Zusätzliche Isolation auf Kunden- und Kursebene innerhalb eines Mandanten
- Versehen der Datensätze mit Zweckattributen und Datenfeldern
- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder nach Ablauf der gesetzlichen Löschfrist, wenn möglich, zu anonymisieren bzw. pseudonymisieren
- Clientseitige Datenisolation: automatisches Löschen aller lokalen Daten bei Mandanten-, Kurs- oder Benutzerwechsel

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- E-Mail-Verschlüsselung (Transportverschlüsselung via TLS)

- WLAN-Verschlüsselung (WPA2 oder höher mit starkem Passwort)
- Bereitstellung von Daten ausschließlich über verschlüsselte Verbindungen: alle API-Kommunikation, Asset-Auslieferung und Webhook-Aufrufe erfolgen ausschließlich über HTTPS/TLS in der Produktivumgebung
- Kryptographisch signierte Anfragen für sicherheitskritische Vorgänge (z. B. Zahlungsauslösung) mit serverseitiger Validierung und Schutz gegen Manipulation und Replay-Angriffe
- Authentifizierungstoken werden nach einmaliger Verwendung automatisch aus der Browser-URL entfernt, um unbeabsichtigte Weitergabe zu verhindern
- Sichere Cookie-Konfiguration im Dashboard: ausschließlich über HTTPS, mit CSRF-Schutz
- Hosting personenbezogener Daten und statischer Assets ausschließlich innerhalb der EU

2.2. Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Aufbewahrung von Formularen, deren Daten in automatisierte Verarbeitungen übernommen worden sind
- Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- Umfassendes Audit-Logging aller sicherheits- und datenschutzrelevanten Ereignisse
- Datenschutzfreundliche Protokollierung: IP-Adressen werden ausschließlich als kryptographischer Hash mit regelmäßiger Schlüsselrotation gespeichert
- Rollenbasierte Audit-Ansichten: Mandanten, Unternehmen, Nutzer und Administratoren sehen jeweils nur die für sie relevanten Protokolleinträge
- Nachverfolgung der E-Mail-Zustellung
- Protokollierung aller Abmeldevorgänge mit Grundangabe

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Verantwortlichen stets verfügbar sind:

- Regelmäßige automatisierte Datenbank-Backups sowie Code-Backups

- Hosting mit professionellem Cloud-Anbieter innerhalb der EU
- Automatische Wiederverbindungs-Mechanismen bei Netzwerkunterbrechungen
- Graceful Degradation: nutzerfreundliche Statusanzeige bei vorübergehender Nichterreichbarkeit des Backends

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Bestellung der Datenschutzbeauftragten Aurea Kindshofer
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)

4.2. Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen gegenüber dem Verantwortlichen entsprechend § 6 dieser Vereinbarung
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Automatische Erkennung und Protokollierung von Sicherheitsereignissen im Audit-Log
- Monitoring der E-Mail-Zustellung mit automatischer Fehlererkennung
- Automatische Session-Invalidierung bei erkannten Sicherheitsvorfällen

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die folgenden implementierten Maßnahmen tragen den Voraussetzungen der Prinzipien „Privacy by Design“ und „Privacy by Default“ Rechnung:

- Schulung der Mitarbeiter in „Privacy by Design“ und „Privacy by Default“
- Umsetzung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO): Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Session-Daten der Kursteilnehmer werden ausschließlich im flüchtigen Speicher gehalten und bei Schließung des Browser-Tabs automatisch gelöscht
- Authentifizierungstoken werden nach einmaliger Verwendung automatisch aus der Browser-URL entfernt
- Passwortlose Authentifizierung für Kursteilnehmer: es ist keine Speicherung von Passwörtern auf Seiten der Endnutzer erforderlich
- IP-Adressen werden im Audit-Log ausschließlich als kryptographischer Hash gespeichert, nicht im Klartext
- DSGVO-konforme Löschfunktion. Löschvorgänge werden mit Löschgrund und Zeitpunkt protokolliert
- Eingabevalidierung: serverseitige Validierung aller Eingaben über typsichere Schemata zur Verhinderung von Injection-Angriffen; kryptographisch signierte Anfragen zur Integritätssicherung

4.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Schriftliche Weisungen an den Auftragsverarbeiter oder Weisungen in Textform (z. B. durch Auftragsverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z. B. durch Anfrage entsprechender Bestätigungen
- Bestätigung von Unterauftragsverarbeitern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)
- Sorgfältige Auswahl von Unterauftragsverarbeitern (insbesondere hinsichtlich Datensicherheit)