Rechtliches

Vereinbarung zur Auftragsverarbeitung

Version 1.3 · Stand: 1. Oktober 2026

nach Art. 28 Abs. 3 DSGVO für die Nutzung des ONYX LMS

zwischen

dem Kunden gemäß Bestellung bzw. Hauptvertrag über die Nutzung des ONYX LMS
– nachfolgend „Verantwortlicher“ –

und

Onyx Consulting GmbH, Abraham-Lincoln-Straße 44, 65189 Wiesbaden, vertreten durch die Geschäftsführer Nicolai Wahl und Jasmin Wahl
– nachfolgend „Auftragsverarbeiter“ –

– gemeinsam „Parteien“ –

Hinweis zur Einbeziehung. Diese Vereinbarung wird Bestandteil des Vertrags über die Nutzung des ONYX LMS („Hauptvertrag“), indem der Verantwortliche sie im Bestellvorgang akzeptiert (Art. 28 Abs. 9 DSGVO, elektronisches Format). Die Vereinbarung ist im Bestellformular verlinkt und vor Abschluss der Bestellung dort einsehbar; mit Absenden der Bestellung wird sie Vertragsbestandteil. Die akzeptierte Fassung wird mit der Bestellung gespeichert und steht dem Verantwortlichen anschließend im Administrationsbereich des LMS unter „Verträge & Datenschutz“ zur Verfügung, ebenso die aktuelle Liste der Unterauftragsverarbeiter (Anlage 3). Vor der Bestellung übermittelt der Auftragsverarbeiter Interessenten diese Liste auf Anfrage an datenschutz@onyx-consulting.de in Textform. Fragen zur Vereinbarung beantwortet der Auftragsverarbeiter unter datenschutz@onyx-consulting.de. Auf Wunsch stellt der Auftragsverarbeiter ein von beiden Parteien unterzeichnetes Exemplar bereit.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen das ONYX LMS als Software-as-a-Service bereit: eine Wissensplattform, über die der Verantwortliche seinen Beschäftigten Kurse für Pflichtunterweisungen zum Abruf bereitstellt und die Teilnahme dokumentiert. Im Rahmen dieser Leistung verarbeitet der Auftragsverarbeiter personenbezogene Daten der Beschäftigten des Verantwortlichen in dessen Auftrag. Diese Vereinbarung gilt nur, soweit der Verantwortliche Daten von Beschäftigten oder anderen Dritten über das LMS verarbeiten lässt; nutzt der Kunde das LMS ausschließlich für sich selbst, findet sie keine Anwendung und es gelten allein die AGB und die Datenschutzerklärung.

(2) Gegenstand, Art, Zweck und Umfang der Verarbeitung, die Kategorien der Daten und der betroffenen Personen ergeben sich aus dem Hauptvertrag, der Konfiguration des LMS durch den Verantwortlichen sowie aus Anlage 1 (Verarbeitungsbeschreibung).

(3) Die im LMS gespeicherten Daten werden ausschließlich in der Bundesrepublik Deutschland verarbeitet. Eine Übermittlung personenbezogener Daten in ein Drittland außerhalb der EU/des EWR erfolgt nur an Unterauftragsverarbeiter, die in der Liste nach Anlage 3 mit dem jeweiligen Verarbeitungsort aufgeführt sind, und nur unter den Voraussetzungen der Art. 44 ff. DSGVO; im Übrigen ist sie nur mit vorheriger Zustimmung des Verantwortlichen in Textform zulässig.

(4) Diese Vereinbarung beginnt mit Freischaltung des Zugangs zum LMS und endet mit der vollständigen Löschung der personenbezogenen Daten nach § 10. Sie gilt über das Ende des Hauptvertrags hinaus, solange der Auftragsverarbeiter noch personenbezogene Daten des Verantwortlichen verarbeitet.

---

§ 2 Verantwortlichkeit und Weisungen

(1) Der Verantwortliche ist im Sinne des Art. 4 Nr. 7 DSGVO allein für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er entscheidet, welche Beschäftigten im LMS angelegt werden, welche Kurse ihnen zugewiesen werden und welche Fristen und Erinnerungen gelten.

(2) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich im Rahmen des Hauptvertrags und nach dokumentierten Weisungen des Verantwortlichen, es sei denn, er ist nach dem Recht der EU oder eines Mitgliedstaats zu einer anderen Verarbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet. Eine Verarbeitung für eigene Zwecke, insbesondere zu Analyse-, Werbe- oder Produktentwicklungszwecken anhand personenbezogener Daten, ist ausgeschlossen.

(3) Als Weisungen gelten der Hauptvertrag, diese Vereinbarung und die Einstellungen, die der Verantwortliche oder seine berechtigten Administratoren im LMS selbst vornehmen (insbesondere Anlegen, Ändern und Löschen von Nutzern, Zuweisung von Kursen, Fristen, Erinnerungen, Exporte). Darüber hinausgehende Einzelweisungen erteilt der Verantwortliche in Textform an datenschutz@onyx-consulting.de. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Er darf die Ausführung der Weisung bis zur Bestätigung oder Änderung durch den Verantwortlichen aussetzen.

(5) Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, gelten als Antrag auf Leistungsänderung und können vergütungspflichtig sein.

§ 3 Pflichten des Auftragsverarbeiters

(1) Vertraulichkeit. Der Auftragsverarbeiter setzt für die Verarbeitung nur Beschäftigte ein, die zur Vertraulichkeit verpflichtet und mit den für sie relevanten Datenschutzvorschriften vertraut gemacht wurden. Die Verpflichtung besteht nach Beendigung der Tätigkeit fort. Der Nachweis der Verpflichtung wird dem Verantwortlichen auf Anfrage erbracht.

(2) Datenschutzbeauftragter. Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt: Andreas Braun, BRAUN Unternehmensdienstleistungen, Abraham-Lincoln-Straße 44, 65189 Wiesbaden, Andreas.Braun@braun-beratung.de. Ein Wechsel wird dem Verantwortlichen mitgeteilt.

(3) Kontaktstelle. Für Weisungen, Betroffenenanfragen, Meldungen von Datenschutzverletzungen und alle sonstigen datenschutzrechtlichen Belange steht das Postfach datenschutz@onyx-consulting.de zur Verfügung; es wird an Werktagen (Montag bis Freitag, ausgenommen gesetzliche Feiertage in Hessen) gelesen. Die weisungsberechtigten und -empfangenden Personen sind in Anlage 4 benannt.

(4) Verarbeitungsverzeichnis. Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

(5) Zusammenarbeit mit Aufsichtsbehörden. Der Auftragsverarbeiter arbeitet auf Anfrage mit der Aufsichtsbehörde zusammen und informiert den Verantwortlichen unverzüglich über Kontrollhandlungen oder Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Verarbeitung beziehen.

(6) Unterstützung. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(7) Trennung. Die Daten des Verantwortlichen werden logisch von den Daten anderer Kunden getrennt verarbeitet (Mandantentrennung).

(8) Keine Kopien. Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Ausgenommen sind Sicherungskopien nach Anlage 2 sowie Daten, die zur Einhaltung gesetzlicher Aufbewahrungspflichten des Auftragsverarbeiters erforderlich sind.

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Die Maßnahmen berücksichtigen den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dem Verantwortlichen in Textform mitgeteilt; die aktuelle Fassung der Anlage 2 ist jederzeit im Administrationsbereich des LMS abrufbar.

(3) Der Auftragsverarbeiter überprüft die Wirksamkeit der Maßnahmen regelmäßig, mindestens jährlich, sowie anlassbezogen.

---

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt eine allgemeine Genehmigung für die Einschaltung der Unterauftragsverarbeiter, die in der Liste nach Anlage 3 zum Zeitpunkt der Bestellung aufgeführt sind. Unterauftragsverhältnisse im Sinne dieser Regelung sind nur solche, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nebenleistungen ohne Zugriff auf personenbezogene Daten (z. B. Telekommunikation, Reinigung, Entsorgung, Wartung ohne Datenzugriff) sind keine Unterauftragsverhältnisse.

(2) Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem dieselben Datenschutzpflichten auferlegt, die in dieser Vereinbarung festgelegt sind. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Einhaltung der Pflichten durch den Unterauftragsverarbeiter.

(3) Beabsichtigt der Auftragsverarbeiter, einen neuen Unterauftragsverarbeiter einzusetzen oder einen bestehenden zu ersetzen, informiert er den Verantwortlichen mindestens vier Wochen vorher in Textform an die im LMS hinterlegte Administrator-Adresse und stellt die aktualisierte Liste der Unterauftragsverarbeiter (Anlage 3) im Administrationsbereich des LMS bereit. Der Verantwortliche kann der Änderung innerhalb von vier Wochen nach Zugang der Mitteilung aus wichtigem datenschutzrechtlichen Grund in Textform widersprechen. Widerspricht er nicht, gilt die Änderung als genehmigt. Bei begründetem Widerspruch bemühen sich die Parteien um eine einvernehmliche Lösung; gelingt dies nicht, kann jede Partei den Hauptvertrag mit einer Frist von vier Wochen kündigen. Bereits gezahlte Entgelte werden für den nicht genutzten Zeitraum anteilig erstattet.

(4) Der Zahlungsdienstleister Stripe Payments Europe, Ltd. verarbeitet ausschließlich Vertrags-, Rechnungs- und Zahlungsdaten des Verantwortlichen selbst und keine Daten der Beschäftigten. Er ist kein Unterauftragsverarbeiter im Sinne dieser Vereinbarung.

---

§ 6 Rechte der betroffenen Personen

(1) Der Verantwortliche kann die Rechte der betroffenen Personen auf Auskunft, Berichtigung und Einschränkung selbst über die Administrationsfunktionen des LMS erfüllen (Einsicht in Nutzerdaten und Nachweise, Bearbeitung von Stammdaten, Deaktivierung von Nutzern, Export als PDF/CSV). Nutzer, die sich noch nie angemeldet haben, kann der Verantwortliche selbst endgültig löschen. Die endgültige

Löschung aller übrigen Nutzer einschließlich zugehöriger Nachweisdateien veranlasst der Auftragsverarbeiter auf Anforderung des Verantwortlichen in Textform an datenschutz@onyx-consulting.de innerhalb von fünf Werktagen und bestätigt die Löschung. Bei sonstigen Ersuchen unterstützt der Auftragsverarbeiter den Verantwortlichen innerhalb derselben Frist mit geeigneten technischen und organisatorischen Maßnahmen.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Ersuchen innerhalb von drei Werktagen an den Verantwortlichen weiter und verweist die betroffene Person an den Verantwortlichen. Der Auftragsverarbeiter beantwortet solche Ersuchen nicht selbst, es sei denn, der Verantwortliche weist ihn in Textform dazu an.

(3) Der Verantwortliche wird darauf hingewiesen, dass die endgültige Löschung eines Nutzers auch dessen Teilnahmebestätigungen und Nachweisdateien löscht; Gegenzeichnungen bleiben mit dem Namen der Person als Bestandteil der betrieblichen Dokumentation erhalten. Nachweise, die der Verantwortliche zur Erfüllung eigener Aufbewahrungspflichten benötigt, sind vor der Löschung zu exportieren.

---

§ 7 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, unverzüglich, spätestens 24 Stunden nachdem sie ihm bekannt geworden ist, an die im LMS hinterlegte Administrator-Adresse. Begründete Verdachtsfälle sind ebenfalls mitzuteilen.

(2) Die Meldung enthält, soweit bekannt: die Art der Verletzung, die Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen oder vorgeschlagenen Abhilfemaßnahmen sowie einen Ansprechpartner. Informationen, die zum Zeitpunkt der Erstmeldung nicht vorliegen, werden ohne unangemessene Verzögerung nachgereicht.

(3) Der Auftragsverarbeiter ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen und stimmt sich hierzu mit dem Verantwortlichen ab. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen obliegen dem Verantwortlichen.

---

§ 8 Nachweis- und Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind. Der Nachweis erfolgt vorrangig durch die Vorlage von Dokumenten: die aktuelle Fassung der Anlage 2, das Zertifikat des Rechenzentrums (ISO/IEC 27001), die Vereinbarungen zur Auftragsverarbeitung mit den Unterauftragsverarbeitern nach Anlage 3 sowie Berichte oder Testate des Datenschutzbeauftragten oder unabhängiger Prüfer.

(2) Reicht der dokumentarische Nachweis im Einzelfall begründet nicht aus, kann der Verantwortliche oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer, der nicht Wettbewerber des Auftragsverarbeiters ist, eine Überprüfung in den Geschäftsräumen des Auftragsverarbeiters durchführen. Die Überprüfung ist mindestens vier Wochen vorher in Textform anzukündigen, findet zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs statt und beschränkt sich auf die Verarbeitung der Daten des Verantwortlichen. Sie soll nicht häufiger als einmal in zwölf Monaten erfolgen, sofern kein konkreter Anlass besteht.

(3) Kontrollen im Rechenzentrum richten sich nach den Zutrittsregelungen des Rechenzentrumsbetreibers; der Auftragsverarbeiter wirkt an der Ermöglichung mit.

(4) Aufwände des Auftragsverarbeiters für Kontrollen ohne konkreten Anlass, die über die Vorlage vorhandener Dokumente hinausgehen, kann der Auftragsverarbeiter nach den Stundensätzen des Hauptvertrags bzw. seiner Preisliste in Rechnung stellen.

---

§ 9 Datenschutz-Folgenabschätzung und vorherige Konsultation

Ist der Verantwortliche zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) oder zur vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DSGVO) verpflichtet, stellt der Auftragsverarbeiter die hierfür erforderlichen Informationen über die Verarbeitung im LMS zur Verfügung. Der Verantwortliche wird darauf hingewiesen, dass die Protokollierung von Abrufen und Fristen durch das LMS eine technische Einrichtung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG sein kann; die Beteiligung des Betriebsrats obliegt dem Verantwortlichen.

---

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Nach Ende des Hauptvertrags wird der Mandant des Verantwortlichen für 90 Tage in einen Lesezugriff versetzt. In diesem Zeitraum stehen dem Verantwortlichen die Exportfunktionen des LMS (Nutzerlisten, Kursabschlüsse, Nachweis-Log, Fristen und Audit-Log als CSV; Teilnahmebestätigungen, Berichte und Sammellisten als PDF; Jahresnachweise als ZIP) weiterhin zur Verfügung; ein Abruf von Inhalten ist nicht mehr möglich. Der Auftragsverarbeiter weist den Verantwortlichen 30 Tage und 7 Tage vor Ablauf der Lizenz sowie mit Beginn des Lesezugriffs per E-Mail an die hinterlegte Administrator-Adresse auf das Vertragsende und die Exportmöglichkeit hin.

(2) Nach Ablauf der 90 Tage löscht der Auftragsverarbeiter innerhalb von weiteren 14 Tagen den Mandanten des Verantwortlichen einschließlich aller personenbezogenen Daten und Nachweisdateien aus den Produktivsystemen und protokolliert die Löschung mit Zeitpunkt und ausführender Person. Auf Anfrage erhält der Verantwortliche eine Löschbestätigung.

(3) Sicherungskopien werden täglich erstellt, verschlüsselt gespeichert und nach 30 Tagen durch Rotation überschrieben. Daten in Sicherungskopien werden nicht gesondert gelöscht; sie sind spätestens 30 Tage nach der Löschung aus dem Produktivsystem, mithin spätestens 135 Tage nach

Vertragsende, vollständig entfernt. Eine Wiederherstellung aus Sicherungskopien erfolgt nach Vertragsende nicht.

(4) Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters (insbesondere für Vertrags- und Rechnungsdaten des Verantwortlichen nach § 257 HGB, § 147 AO) bleiben unberührt; sie betreffen keine Daten der Beschäftigten.

(5) Der Verantwortliche kann jederzeit während der Vertragslaufzeit die Löschung einzelner Nutzer oder des gesamten Mandanten verlangen bzw. im LMS selbst veranlassen. Die Aufbewahrung von Teilnahmenachweisen zur Erfüllung eigener gesetzlicher Pflichten obliegt dem Verantwortlichen.

---

§ 11 Haftung

(1) Die Haftung der Parteien im Innenverhältnis richtet sich nach den Haftungsregelungen des Hauptvertrags. Art. 82 DSGVO bleibt im Außenverhältnis zu den betroffenen Personen unberührt.

(2) Der Auftragsverarbeiter haftet für Schäden, die durch eine nicht weisungsgemäße oder gegen diese Vereinbarung verstoßende Verarbeitung verursacht wurden. Der Verantwortliche haftet für die Rechtmäßigkeit der Datenerhebung und -übermittlung an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der von ihm erteilten Weisungen.

---

§ 12 Schlussbestimmungen

(1) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen die Regelungen dieser Vereinbarung in datenschutzrechtlichen Fragen vor.

(2) Änderungen und Ergänzungen bedürfen der Textform. Der Auftragsverarbeiter kann die Anlagen 2 und 3 nach Maßgabe der §§ 4 und 5 aktualisieren.

(3) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand ist, soweit gesetzlich zulässig, Wiesbaden.

(5) Die Einrede des Zurückbehaltungsrechts nach § 273 BGB ist hinsichtlich der im Auftrag verarbeiteten Daten ausgeschlossen.

Stand: 1. Oktober 2026 · Version 1.3

Anlage 1 – Beschreibung der Verarbeitung

1. Gegenstand und Zweck

Bereitstellung des ONYX LMS (Software-as-a-Service) zur Verteilung von Kursen für Pflichtunterweisungen (z. B. Datenschutz, IT-Sicherheit, KI im Unternehmen, Fahrsicherheit, Bildschirmarbeit, Arbeitssicherheit) an Beschäftigte des Verantwortlichen sowie zur Dokumentation der Teilnahme. Zweck ist die Unterstützung des Verantwortlichen bei der Erfüllung seiner Unterweisungs- und Nachweispflichten (u. a. § 12 ArbSchG, DGUV Vorschrift 1, Art. 39 Abs. 1 lit. b DSGVO, Art. 4 Verordnung (EU) 2024/1689). Die Unterweisung selbst und ihre Wirksamkeitskontrolle obliegen dem Verantwortlichen; das LMS führt keine Prüfungen durch, bewertet keine Lernergebnisse und speichert keine Antworten auf freiwillige Reflexionsfragen.

2. Art der Verarbeitung

Erheben (Anlegen von Nutzern durch den Verantwortlichen, CSV-Import), Speichern, Organisieren (Gruppen, Zuweisungen), Auslesen, Übermitteln an den Verantwortlichen (Exporte, Berichte, Benachrichtigungen), Löschen.

3. Kategorien betroffener Personen

- Beschäftigte des Verantwortlichen, denen Zugang zum LMS gewährt wird, sowie sonstige Personen, für die der Verantwortliche aufgrund eigener gesetzlicher Unterweisungspflicht verantwortlich ist (z. B. in seinem Betrieb eingesetzte Leiharbeitnehmer)
- Administratoren und verantwortliche Personen des Verantwortlichen (z. B. Gegenzeichnende bei Fahrsicherheit)

4. Kategorien personenbezogener Daten

Kategorien personenbezogener Daten und die jeweils verarbeiteten Angaben

Kategorie	Daten
Stammdaten	Vorname, Nachname, geschäftliche E-Mail-Adresse, Gruppe, Rolle im LMS (Administrator, verantwortliche Person, Nutzer), Status (aktiv/deaktiviert) sowie das Merkmal „Führerschein vorhanden“ (ja/nein) für die Zuweisung des Kurses Fahrsicherheit. Weitere Angaben zur Person (z. B. Personalnummer, Telefonnummer, Geburtsdatum) werden nicht erhoben.
Authentifizierungsdaten	Passwort-Hash und Zwei-Faktor-Geheimnis bei lokaler Anmeldung.
Nutzungsdaten	Zeitpunkt der Anmeldung, Zeitpunkt und Status des Abrufs je Kurs und Abschnitt, gesetzte Bearbeitungsfristen, versendete Erinnerungen

Kategorie	Daten
Nachweisdaten	Teilnahmebestätigungen (Name, Zeitpunkt, Kursversion, Nachweisnummer); bei Fahrsicherheit: Bestätigung der teilnehmenden Person und Gegenzeichnung der verantwortlichen Person, jeweils nur im angemeldeten Zustand, mit Konto-ID, eingetragenem Namen, Zeitstempel und Wortlaut zum Zeitpunkt der Bestätigung, sowie freiwillige Angaben zur betrieblichen Ergänzung. IP-Adressen und Browserkennungen werden bei Nachweisen nicht gespeichert und nicht auf den Nachweis gedruckt; der Nachweis trägt eine Nachweis-ID zur Zuordnung.
Protokolldaten	Server-Logfiles des Webservers und Anwendungslog (IP-Adresse, Zeitpunkt, aufgerufene Ressource, User-Agent) zur Sicherstellung des Betriebs und zur Abwehr von Angriffen, Aufbewahrung 14 Tage. Anmeldeprotokoll (erfolgreiche und fehlgeschlagene Anmeldungen, mit Konto, Zeitpunkt, IP-Adresse und User-Agent) zur Erkennung und Aufklärung von Sicherheitsvorfällen, Aufbewahrung 90 Tage. Audit-Log der Plattform (Kursaktivität und Verwaltungsereignisse mit Konto, Zeitpunkt und Aktion, ohne IP-Adresse und User-Agent), Aufbewahrung 730 Tage, für den Verantwortlichen als CSV abrufbar. Mail-Versandprotokoll (Empfänger, Betreff, Zeitpunkt, Zustellstatus; ohne Nachrichteninhalt) 180 Tage; Webhook-Zustellprotokoll (Nutzdaten, ohne Beschäftigtendaten) 90 Tage; Sitzungsdaten (Sitzungskennung, ohne IP-Adresse) für die Dauer der Sitzung, Ablauf nach 120 Minuten Inaktivität.
Kommunikationsdaten	Inhalt und Zeitpunkt systemseitiger E-Mails (Einladung, Erinnerung, Fristhinweis) sowie Nachrichten innerhalb der Plattform

Nicht Gegenstand dieser Vereinbarung: Firmen-, Ansprechpartner-, Rechnungs- und Zahlungsdaten des Verantwortlichen selbst (Firma, Ansprechperson, E-Mail, optional Telefon, Rechnungsadresse, USt-IdNr.), die im Bestellvorgang erhoben werden. Insoweit ist der Auftragsverarbeiter eigener Verantwortlicher; es gilt die Datenschutzerklärung unter onyx-lms.de/datenschutz.

Nicht verarbeitet werden: besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, Daten zu strafrechtlichen Verurteilungen (Art. 10 DSGVO), Prüfungs- oder Leistungsergebnisse, Antworten auf Reflexionsfragen, private Kontaktdaten. Der Verantwortliche ist verpflichtet, solche Daten nicht in Freitextfelder, Gruppenbezeichnungen oder Importdateien einzutragen.

5. Whitelabel-Konfiguration

Bei Nutzung der Whitelabel-Option hinterlegt der Verantwortliche Logo, Farben, Texte und eine Subdomain (firma.onyx-lms.de). Diese Angaben enthalten keine personenbezogenen Daten der Beschäftigten. Das TLS-Zertifikat für die Subdomain stellt der Auftragsverarbeiter aus.

6. Verarbeitungsort

Die im LMS gespeicherten Daten werden ausschließlich in der Bundesrepublik Deutschland (Wiesbaden) verarbeitet. In einzelnen Kursen sind Videos eines externen Videodienstes eingebunden; beim Aufruf solcher Kursabschnitte wird die IP-Adresse der nutzenden Person an den Anbieter des Videodienstes

übermittelt, der die Daten auch außerhalb der EU/des EWR verarbeiten kann. Anbieter, Verarbeitungsort und Grundlage der Übermittlung ergeben sich aus der Liste nach Anlage 3 (§ 1 Abs. 3).

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die Maßnahmen gliedern sich in Maßnahmen der Infrastruktur (verantwortet durch einen IT-Dienstleister als Unterauftragsverarbeiter, mit Rechenzentrum in Wiesbaden) und Maßnahmen der Anwendung ONYX LMS (verantwortet durch den Auftragsverarbeiter). Die Namen der Unterauftragsverarbeiter enthält die Liste nach Anlage 3.

A. Infrastruktur (IT-Dienstleister mit Rechenzentrum in Wiesbaden)

Maßnahmen der Infrastruktur und ihre Umsetzung

Maßnahme	Umsetzung
Rechenzentrum	Colocation in einem Rechenzentrum in Wiesbaden, zertifiziert nach ISO/IEC 27001. Zutritt nur für festgelegte Personen: Quittierung der Schlüsselausgabe und Transponder durch Wachpersonal, Protokollierung des Zugangs, PIN-Eingabe, Sicherheitstüren, Videoüberwachung
Serverbetrieb	Bereitstellung und Betrieb eines dedizierten virtuellen Servers für das ONYX LMS durch den IT-Dienstleister; personalisierte Administrationszugänge, Zwei-Faktor-Authentifizierung, Protokollierung von Administratorzugriffen, Zugriff ausschließlich über verschlüsselte VPN-Verbindung; keine Fernwartungswerkzeuge Dritter auf dem Server
Netzwerk	Firewall, Virenschutz auf Serversystemen, automatisierte Überwachung und Alarmierung, Transportverschlüsselung (TLS) für alle Verbindungen
Verfügbarkeit	Redundante Server- und Stromversorgungssysteme (USV), Backup-Systeme in getrenntem Brandabschnitt, regelmäßige Wiederherstellungstests
Datensicherung	Tägliche Sicherung (nachts), verschlüsselt, Aufbewahrung 30 Tage mit anschließender Rotation; Wiederherstellung durch verschiedene IT-Mitarbeiter möglich
Patch-Management	Zentral automatisierte Einspielung von Betriebssystem-Sicherheitsupdates; regelmäßige Prüfung, ob Software, Firewall und Virenschutz aktuell sind
Datenträger	Festplattenverschlüsselung; sichere Löschung bzw. physische Vernichtung ausgemusterter Datenträger
Organisation	Externer Datenschutzbeauftragter, Verpflichtung aller Mitarbeiter auf Vertraulichkeit, Verfahrensverzeichnis, regelmäßige und teils unangekündigte Überprüfung der Maßnahmen

Maßnahme	Umsetzung
Vertragliche Absicherung	Vereinbarung zur Auftragsverarbeitung zwischen der Onyx Consulting GmbH und dem IT-Dienstleister mit TOM-Anlage; wird dem Verantwortlichen auf Anfrage vorgelegt

B. Anwendung ONYX LMS (Onyx Consulting GmbH)

Maßnahmen der Anwendung ONYX LMS und ihre Umsetzung

Maßnahme	Umsetzung
Mandantentrennung	Gemeinsame Datenbank mit Mandantenkennung an jedem Datensatz; die Mandantenzugehörigkeit wird auf Anwendungsebene bei jedem Zugriff erzwungen (Global Scope), sodass Daten anderer Mandanten technisch nicht abrufbar sind
Rollen- und Rechtekonzept	Rollen: Administrator, verantwortliche Person (Gegenzeichnung, nur eigene Abteilungen), Nutzer. Rechte nach dem Need-to-know-Prinzip; Administratoren des Verantwortlichen sehen nur den eigenen Mandanten. Mitarbeiter des Auftragsverarbeiters greifen nur zu Support- und Betriebszwecken über gesonderte Super-Administrator-Konten auf Kundendaten zu; Anmeldungen und administrative Aktionen dieser Konten werden personenbezogen protokolliert
Authentifizierung	Lokale Anmeldung mit Mindestpasswortlänge von 10 Zeichen (Buchstaben und Ziffern), Anmeldeversuche gedrosselt auf 6 Versuche pro Minute, Passwörter ausschließlich als bcrypt-Hash gespeichert; Zwei-Faktor-Authentifizierung per Authenticator-App für alle Verwaltungskonten verpflichtend
Transportverschlüsselung	Ausschließlich HTTPS (TLS 1.2 oder höher), HSTS aktiviert, Session-Cookies mit den Attributen Secure, HttpOnly und SameSite
Verschlüsselung ruhender Daten	Datenbank und Dateisystem auf verschlüsselten Datenträgern (Infrastruktur); Sicherungskopien verschlüsselt
Pseudonymisierung	Nachweise werden ohne IP-Adresse und Browserkennung erzeugt und gespeichert; die Zuordnung erfolgt über eine Nachweis-ID und die Konto-ID
Protokollierung	Audit-Log für Verwaltungsereignisse (Anlegen/Ändern/Löschen von Nutzern, Zuweisungen, Gegenzeichnungen) mit Zeitstempel und handelnder Person; Nachweisdaten nach Bestätigung unveränderlich; Kurse mit Nachweisen können nur archiviert, nicht gelöscht werden
Eingabekontrolle	Änderungen an Nutzer- und Nachweisdaten sind im Audit-Log nachvollziehbar; Import per CSV nur durch Administratoren

Maßnahme	Umsetzung
Löschkonzept	Deaktivierung und – bei nie angemeldeten Personen – Löschung einzelner Nutzer durch den Administrator des Verantwortlichen; endgültige Löschung übriger Nutzer einschließlich Nachweisdateien durch den Auftragsverarbeiter auf Anforderung; Lesezugriff 90 Tage nach Vertragsende, danach Löschung des Mandanten einschließlich aller Dateien mit Protokolleintrag innerhalb von 14 Tagen; Server- und Anwendungslogs nach 14 Tagen; Anmeldeprotokoll nach 90 Tagen; Audit-Log (ohne IP/User-Agent) nach 730 Tagen; Mail-Protokoll nach 180 Tagen; Webhook-Protokoll nach 90 Tagen; Backup-Rotation nach 30 Tagen
Trennung von Umgebungen	Getrennte Staging- und Produktivumgebung; Staging ohne Produktivdaten und mit Zugangsschutz
Entwicklung und Betrieb	Versionskontrolle; Code-Review im Vier-Augen-Prinzip vor jeder Produktivsetzung; automatisierte Prüfung der Abhängigkeiten auf bekannte Sicherheitslücken (composer audit / Dependabot); sicherheitsrelevante Updates werden priorisiert eingespielt
Datenschutz durch Voreinstellung	Nutzerkonten beschränken sich auf Name, geschäftliche E-Mail, Gruppe, Rolle und das Merkmal „Führerschein vorhanden“; keine weiteren Personenfelder; Reflexionsfragen werden nicht gespeichert; keine Analyse- oder Marketing-Tracker des Auftragsverarbeiters in der Anwendung
Organisation	Verpflichtung aller Beschäftigten der Onyx Consulting GmbH auf Vertraulichkeit; externer Datenschutzbeauftragter; jährliche Überprüfung dieser Anlage; Prozess zur Meldung von Datenschutzverletzungen mit 24-Stunden-Frist über datenschutz@onyx-consulting.de

Anlage 3 – Unterauftragsverarbeiter

(1) Die aktuelle Liste der Unterauftragsverarbeiter mit Name, Anschrift, Leistung, Art des Datenzugriffs, Verarbeitungsort und, bei Verarbeitung außerhalb der EU/des EWR, der Grundlage der Übermittlung ist für den Verantwortlichen nach Vertragsschluss im Kundenbereich des ONYX LMS (Administrationsbereich „Verträge & Datenschutz“) einsehbar. Vor der Bestellung erhalten Interessenten die Liste auf Anfrage an datenschutz@onyx-consulting.de in Textform. Die zum Zeitpunkt der Bestellung dort aufgeführten Unterauftragsverarbeiter gelten als genehmigt (§ 5 Abs. 1).

(2) Über beabsichtigte Änderungen der Liste informiert der Auftragsverarbeiter den Verantwortlichen vorab in Textform; Frist, Widerspruchsrecht und Folgen eines Widerspruchs richten sich nach § 5 Abs. 3 (Art. 28 Abs. 2 Satz 2 DSGVO).

(3) Nicht als Unterauftragsverarbeiter beteiligt ist der Zahlungsdienstleister Stripe Payments Europe, Ltd. (nur Vertrags- und Zahlungsdaten des Verantwortlichen, § 5 Abs. 4). Der E-Mail-Versand erfolgt über

einen eigenen Mailserver des Auftragsverarbeiters auf der Infrastruktur des IT-Dienstleisters; ein weiterer Dienstleister ist daran nicht beteiligt.

Anlage 4 – Ansprechpartner und weisungsberechtigte Personen

Rollen und Kontaktstellen für Weisungen, Datenschutzbeauftragten und Meldungen

Rolle	Kontakt
Weisungsberechtigt für den Verantwortlichen	Die im LMS als Administrator hinterlegten Personen sowie die im Bestellvorgang angegebene Ansprechperson; Änderungen über das LMS oder in Textform an datenschutz@onyx-consulting.de
Weisungsempfang beim Auftragsverarbeiter	datenschutz@onyx-consulting.de (werktäglich gelesen); Eskalation an die Geschäftsführung
Datenschutzbeauftragter des Auftragsverarbeiters	Andreas Braun, BRAUN Unternehmensdienstleistungen, Abraham-Lincoln-Straße 44, 65189 Wiesbaden, Andreas.Braun@braun-beratung.de
Meldung von Datenschutzverletzungen an den Verantwortlichen	E-Mail-Adresse des im LMS hinterlegten Hauptadministrators; der Verantwortliche hält diese aktuell