

AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV)

zwischen

Kunde

(Auftraggeber)

und

aurixus GmbH

(Auftragsverarbeiter)

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der Nutzung der Plattform „DigitalCheckIn Education“ sowie der hierzu vereinbarten Leistungen.

(2) Gegenstand der Verarbeitung sind die Erhebung, Speicherung, Organisation, Nutzung, Übermittlung, Bereitstellung, Auswertung, Archivierung, Löschung sowie sonstige Verarbeitungen personenbezogener Daten, soweit dies zur Erbringung der vertraglich vereinbarten Leistungen erforderlich ist.

(3) Art und Zweck der Verarbeitung, die Kategorien betroffener Personen sowie die Kategorien personenbezogener Daten ergeben sich aus Anlage 1 zu dieser Vereinbarung.

(4) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit nicht gesetzliche Verpflichtungen eine abweichende Verarbeitung verlangen.

(5) Die Dauer der Verarbeitung richtet sich nach der Laufzeit des zwischen den Parteien bestehenden Softwarenutzungsvertrages einschließlich etwaiger Nachfolge-, Zusatz- oder Erweiterungsvereinbarungen.

(6) Mit Beendigung des zugrunde liegenden Vertragsverhältnisses enden grundsätzlich auch die Verarbeitungsleistungen des Auftragsverarbeiters. Die Rückgabe, Bereitstellung, Aufbewahrung und Löschung personenbezogener Daten richtet sich nach § 12 dieser Vereinbarung.

(7) Soweit vom Auftraggeber aktivierte Funktionen künstlicher Intelligenz, Automatisierungen oder Analysefunktionen genutzt werden, erfolgt deren Einsatz ausschließlich im Rahmen der vertraglich vereinbarten Leistungen und der Weisungen des Auftraggebers.

§ 2 Art und Zweck der Verarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zum Zweck der Erbringung der zwischen den Parteien vereinbarten Leistungen im Zusammenhang mit der Plattform „DigitalCheckIn Education“ einschließlich der beauftragten Erweiterungsmodule, Integrationen, Kommunikationsdienste und sonstigen Plattformfunktionen.

(2) Die Verarbeitung erfolgt insbesondere zur Unterstützung administrativer, organisatorischer, dokumentationsbezogener, kommunikativer, sicherheitsbezogener und governanceorientierter Prozesse des Auftraggebers.

(3) Die Verarbeitung kann insbesondere folgende Tätigkeiten umfassen:

- a) Verwaltung von Teilnehmern, Benutzern, Dozenten, Prüfern, Ansprechpartnern und sonstigen durch den Auftraggeber verwalteten Personen,
- b) Verwaltung von Kursen, Maßnahmen, Klassen, Gruppen, Standorten und organisatorischen Einheiten,
- c) Erfassung, Verarbeitung und Dokumentation von Anwesenheiten, Check-In- und Check-Out-Vorgängen,
- d) Erfassung, Verarbeitung, Speicherung und Bereitstellung digitaler Signaturen, Anwesenheitsnachweise und sonstiger Dokumentationsnachweise,
- e) Verwaltung von Rollen, Berechtigungen, Benutzerkonten und Authentifizierungsverfahren,
- f) Betrieb, Wartung, Überwachung und Absicherung der Plattform sowie der eingesetzten Hardwarekomponenten,
- g) Erstellung, Verarbeitung und Bereitstellung von Berichten, Auswertungen, Statistiken, Exporten und Nachweisen,
- h) Durchführung von Kommunikations- und Benachrichtigungsprozessen über unterstützte Kommunikationskanäle, insbesondere E-Mail, Microsoft Teams, Push-Benachrichtigungen sowie weitere vom Auftraggeber genutzte Kommunikationsdienste,
- i) Durchführung von Workflow-, Automatisierungs-, Monitoring-, Reporting- und Governancefunktionen im Rahmen der beauftragten Leistungen,
- j) Bereitstellung und Nutzung von Schnittstellen, Integrationen und Identitätsdiensten, insbesondere Microsoft Entra ID, SAML, LDAP, OpenID Connect sowie vergleichbarer Authentifizierungs- und Integrationsdienste,
- k) Fehleranalyse, Support, Fernwartung, Sicherheitsüberwachung und technische Administration der Plattform,
- l) Durchführung von Analyse-, Automatisierungs- und KI-gestützten Funktionen im Rahmen der durch den Auftraggeber aktivierten und beauftragten Leistungen.

(4) Soweit Erweiterungsmodule, Kommunikationsdienste, Automatisierungsfunktionen, Analysefunktionen oder KI-gestützte Funktionen eingesetzt werden, erfolgt die Verarbeitung ausschließlich zur Erbringung der jeweils beauftragten Leistungen.

(5) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nicht für eigene Zwecke und trifft keine eigenständigen Entscheidungen über die Zwecke der Verarbeitung.

(6) Die konkrete Ausgestaltung der Verarbeitung ergibt sich aus dem Softwarenutzungsvertrag, den zugehörigen Anlagen, den jeweils beauftragten Leistungen, den aktivierten Funktionen der Plattform sowie den dokumentierten Weisungen des Auftraggebers.

§ 3 Kategorien betroffener Personen

Von der Verarbeitung personenbezogener Daten können insbesondere folgende Personengruppen betroffen sein:

- a) Teilnehmer von Bildungs-, Schulungs-, Qualifizierungs-, Weiterbildungs- oder sonstigen Maßnahmen des Auftraggebers,
- b) Mitarbeiter des Auftraggebers,
- c) Dozenten, Referenten, Ausbilder und Lehrkräfte,
- d) Prüfer, Bewertungspersonen und sonstige mit Prüfungs- oder Nachweisprozessen betraute Personen,
- e) Administratoren und sonstige Benutzer der Plattform,
- f) Ansprechpartner und Kontaktpersonen des Auftraggebers,
- g) sonstige Personen, die durch den Auftraggeber innerhalb der Plattform verwaltet oder verarbeitet werden.

Die konkrete Verarbeitung richtet sich nach den vom Auftraggeber genutzten Funktionen, Modulen und Anwendungsfällen.

§ 4 Kategorien personenbezogener Daten

Im Rahmen der Auftragsverarbeitung können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

a) Stammdaten

- Vorname
- Nachname
- Benutzername
- Teilnehmernummer
- Personalnummer
- sonstige Identifikationsmerkmale

b) Kontaktdaten

- E-Mail-Adresse
- Telefonnummer
- dienstliche Kontaktinformationen

c) Organisations- und Zuordnungsdaten

- Kurszuordnungen
- Maßnahmenzuordnungen
- Standortzuordnungen
- Gruppen- und Klassenzuordnungen
- Rollen und Berechtigungen

- organisatorische Zuordnungen

d) Anwesenheits- und Nachweisdaten

- Anwesenheitsdaten
- Check-In-Daten
- Check-Out-Daten
- Anwesenheitsnachweise
- Fehlzeiteninformationen
- Zeitstempel

e) Signatur- und Identifikationsdaten

- digitale Signaturen
- Signaturzeitpunkte
- NFC-Tag-IDs
- Kartennummern
- Identifikationsmerkmale im Rahmen der Plattformnutzung

f) Benutzer- und Nutzungsdaten

- Benutzerkonten
- Rolleninformationen
- Berechtigungsinformationen
- Anmeldeinformationen
- Protokoll- und Auditdaten

g) Kommunikationsdaten

- Kommunikationsinhalte
- Benachrichtigungen
- Versandinformationen
- Kommunikationsprotokolle

h) Sonstige durch den Auftraggeber bereitgestellte Daten

- sonstige personenbezogene Daten, die durch den Auftraggeber im Rahmen der vertragsgemäßen Nutzung der Plattform verarbeitet werden.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO ist nicht Gegenstand der vertragsgemäßen Nutzung der Plattform.

(3) Der Auftraggeber ist dafür verantwortlich, keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO zu verarbeiten, soweit dies nicht ausdrücklich zwischen den Parteien vereinbart wurde.

(4) Die konkrete Verarbeitung richtet sich nach den vom Auftraggeber genutzten Funktionen, Erweiterungsmodulen und Anwendungsfällen.

§ 5 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO).

(2) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sowie für die Wahrung der Rechte betroffener Personen verantwortlich.

(3) Der Auftraggeber bestimmt die Zwecke und Mittel der Verarbeitung im Rahmen der vertraglich vereinbarten Nutzung der Plattform und erteilt dem Auftragsverarbeiter die erforderlichen Weisungen.

(4) Weisungen des Auftraggebers sind grundsätzlich in Textform zu erteilen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(5) Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter unverzüglich zu informieren, wenn er Fehler, Unregelmäßigkeiten oder Verstöße gegen datenschutzrechtliche Vorschriften im Zusammenhang mit der Auftragsverarbeitung feststellt.

(6) Der Auftraggeber ist dafür verantwortlich, dass die von ihm verarbeiteten personenbezogenen Daten sachlich richtig, rechtmäßig erhoben und für die vorgesehenen Zwecke erforderlich sind.

(7) Der Auftraggeber ist verpflichtet, die Plattform ausschließlich im Einklang mit den geltenden datenschutzrechtlichen Vorschriften sowie den vertraglichen Vereinbarungen zu nutzen.

(8) Der Auftraggeber wird den Auftragsverarbeiter unverzüglich informieren, wenn Betroffene ihre Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch geltend machen und die Unterstützung des Auftragsverarbeiters erforderlich ist.

(9) Der Auftraggeber ist dafür verantwortlich, keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO sowie keine sonstigen Daten mit besonderen gesetzlichen Schutzanforderungen zu verarbeiten, soweit dies nicht ausdrücklich zwischen den Parteien vereinbart wurde.

(10) Der Auftraggeber bleibt für die fachliche, organisatorische, rechtliche und datenschutzrechtliche Bewertung der Verarbeitungsergebnisse verantwortlich. Dies gilt auch für Ergebnisse von Automatisierungs-, Analyse- oder KI-gestützten Funktionen der Plattform.

§ 6 Pflichten des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit nicht eine gesetzliche Verpflichtung zur Verarbeitung besteht.
- (2) Der Auftragsverarbeiter wird die zur Verarbeitung personenbezogener Daten befugten Personen vor Aufnahme ihrer Tätigkeit auf Vertraulichkeit verpflichten und über die datenschutzrechtlichen Anforderungen informieren.
- (3) Der Auftragsverarbeiter trifft angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO zum Schutz personenbezogener Daten. Die zum Zeitpunkt des Vertragsschlusses geltenden Maßnahmen ergeben sich aus Anlage 2 (Technische und organisatorische Maßnahmen).
- (4) Der Auftragsverarbeiter ist berechtigt, technische und organisatorische Maßnahmen fortlaufend weiterzuentwickeln, anzupassen oder durch gleichwertige Maßnahmen zu ersetzen, soweit hierdurch das Schutzniveau der Verarbeitung nicht unterschritten wird.
- (5) Der Auftragsverarbeiter unterstützt den Auftraggeber im angemessenen Umfang bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen, soweit dies aufgrund der Art der Verarbeitung erforderlich ist.
- (6) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.
- (7) Der Auftragsverarbeiter führt die Verarbeitung personenbezogener Daten grundsätzlich innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durch. Soweit im Einzelfall eine Verarbeitung außerhalb der EU oder des EWR erfolgt, werden die hierfür erforderlichen datenschutzrechtlichen Voraussetzungen gemäß DSGVO eingehalten.
- (8) Der Auftragsverarbeiter wird personenbezogene Daten nicht für eigene Zwecke verarbeiten, auswerten, vermarkten oder an Dritte weitergeben, soweit dies nicht zur vertragsgemäßen Leistungserbringung erforderlich oder gesetzlich vorgeschrieben ist.
- (9) Soweit Automatisierungs-, Analyse- oder KI-gestützte Funktionen eingesetzt werden, erfolgt deren Nutzung ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen. Der Auftragsverarbeiter trifft keine eigenständigen Entscheidungen mit rechtlicher Wirkung gegenüber betroffenen Personen.
- (10) Der Auftragsverarbeiter dokumentiert datenschutzrechtlich relevante Vorgänge in angemessenem Umfang und stellt dem Auftraggeber die nach Art. 28 DSGVO erforderlichen Informationen auf Anfrage zur Verfügung.

§ 7 Technische und organisatorische Maßnahmen

- (1) Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten sicherzustellen.
- (2) Die zum Zeitpunkt des Vertragsschlusses geltenden technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 2 (Technische und organisatorische Maßnahmen), die Bestandteil dieser Vereinbarung ist.

(3) Die technischen und organisatorischen Maßnahmen dienen insbesondere der Gewährleistung von:

- a) Vertraulichkeit,
- b) Integrität,
- c) Verfügbarkeit,
- d) Belastbarkeit der Systeme und Dienste,
- e) Wiederherstellbarkeit nach Zwischenfällen,
- f) Nachvollziehbarkeit von Verarbeitungsvorgängen,
- g) Schutz vor unbefugtem Zugriff.

(4) Der Auftragsverarbeiter ist berechtigt, technische und organisatorische Maßnahmen fortlaufend an technische, organisatorische, rechtliche oder sicherheitsrelevante Entwicklungen anzupassen oder durch gleichwertige Maßnahmen zu ersetzen, soweit hierdurch das Schutzniveau der Verarbeitung nicht unterschritten wird.

(5) Soweit der Auftragsverarbeiter neue Technologien, Plattformkomponenten, Erweiterungsmodule, Automatisierungsfunktionen oder KI-gestützte Funktionen einführt, wird er angemessene technische und organisatorische Maßnahmen zur Wahrung des Datenschutzes und der Informationssicherheit berücksichtigen.

(6) Auf Verlangen des Auftraggebers stellt der Auftragsverarbeiter Informationen über die wesentlichen technischen und organisatorischen Maßnahmen zur Verfügung, soweit dies zur Erfüllung datenschutzrechtlicher Anforderungen erforderlich ist.

§ 8 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Beauftragung weiterer Auftragsverarbeiter (Unterauftragsverarbeiter) gemäß Art. 28 DSGVO.

(2) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter ergeben sich aus Anlage 3 (Unterauftragsverarbeiter), die Bestandteil dieser Vereinbarung ist.

(3) Der Auftragsverarbeiter ist berechtigt, bestehende Unterauftragsverarbeiter zu ersetzen, zusätzliche Unterauftragsverarbeiter einzusetzen oder Leistungen auf weitere Unterauftragsverarbeiter zu übertragen, soweit dies zur vertragsgemäßen Leistungserbringung erforderlich ist.

(4) Der Auftragsverarbeiter wird den Auftraggeber über die Aufnahme neuer Unterauftragsverarbeiter oder wesentliche Änderungen bestehender Unterauftragsverarbeiter in geeigneter Weise informieren.

(5) Der Auftraggeber kann einer beabsichtigten Änderung innerhalb von 30 Kalendertagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund widersprechen.

(6) Im Falle eines berechtigten Widerspruchs werden die Parteien versuchen, eine einvernehmliche Lösung zu finden. Ist dies nicht möglich und kann der Auftragsverarbeiter die betreffende Leistung ohne den betroffenen Unterauftragsverarbeiter nicht erbringen, steht

beiden Parteien ein außerordentliches Kündigungsrecht hinsichtlich der betroffenen Leistungen zu.

(7) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich zu Datenschutz- und Sicherheitsanforderungen, die den Anforderungen dieser Vereinbarung entsprechen.

(8) Der Auftragsverarbeiter bleibt gegenüber dem Auftraggeber für die ordnungsgemäße Erfüllung der datenschutzrechtlichen Verpflichtungen seiner Unterauftragsverarbeiter verantwortlich.

(9) Soweit Unterauftragsverarbeiter Automatisierungs-, Analyse-, Kommunikations-, Authentifizierungs-, Hosting-, Cloud- oder KI-Dienste bereitstellen, erfolgt deren Einsatz ausschließlich im Rahmen der geltenden datenschutzrechtlichen Vorgaben und der vertraglichen Vereinbarungen zwischen den Parteien.

§ 9 Unterstützung des Auftraggebers

(1) Der Auftragsverarbeiter unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen in angemessenem Umfang bei der Erfüllung seiner datenschutzrechtlichen Pflichten.

(2) Dies umfasst insbesondere die Unterstützung bei:

a) der Bearbeitung von Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch,

b) der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO,

c) der Durchführung von Datenschutz-Folgenabschätzungen,

d) der vorherigen Konsultation von Aufsichtsbehörden, soweit dies erforderlich ist,

e) der Untersuchung und Dokumentation datenschutzrechtlich relevanter Vorfälle.

(3) Erhält der Auftragsverarbeiter Anfragen betroffener Personen unmittelbar, wird er diese unverzüglich an den Auftraggeber weiterleiten, sofern eine Zuordnung zum Auftraggeber möglich ist.

(4) Der Auftragsverarbeiter wird betroffene Personen nicht eigenständig beantworten, soweit er hierzu nicht gesetzlich verpflichtet oder vom Auftraggeber ausdrücklich angewiesen wurde.

(5) Die Unterstützung erfolgt im Rahmen der gesetzlichen Verpflichtungen des Auftragsverarbeiters und der ihm tatsächlich zur Verfügung stehenden technischen und organisatorischen Möglichkeiten.

(6) Soweit die Unterstützung einen erheblichen zusätzlichen Aufwand verursacht und die Ursache nicht vom Auftragsverarbeiter zu vertreten ist, kann der Auftragsverarbeiter hierfür eine angemessene Vergütung nach den jeweils gültigen Vergütungssätzen verlangen. Hierüber wird der Auftraggeber vorab informiert.

(7) Der Auftragsverarbeiter stellt dem Auftraggeber auf Anfrage die Informationen zur Verfügung, die dieser zur Erfüllung seiner Nachweis- und Rechenschaftspflichten nach der DSGVO in angemessenem Umfang benötigt.

§ 10 Kontrollrechte

(1) Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Verpflichtungen des Auftragsverarbeiters in angemessenem Umfang zu überprüfen oder durch einen zur Verschwiegenheit verpflichteten Dritten überprüfen zu lassen.

(2) Der Auftragsverarbeiter wird dem Auftraggeber auf Anfrage die zur Erfüllung der Nachweispflichten nach Art. 28 DSGVO erforderlichen Informationen zur Verfügung stellen.

(3) Der Nachweis kann insbesondere erfolgen durch:

- a) geeignete Dokumentationen,
- b) Sicherheits- und Datenschutzkonzepte,
- c) technische und organisatorische Maßnahmen,
- d) Zertifizierungen,
- e) Prüfberichte,
- f) Selbstauskünfte des Auftragsverarbeiters.

(4) Vor-Ort-Kontrollen sind nur zulässig, soweit berechtigte Zweifel an der Einhaltung der datenschutzrechtlichen Verpflichtungen bestehen und andere Nachweismöglichkeiten nicht ausreichen.

(5) Vor-Ort-Kontrollen sind dem Auftragsverarbeiter mit angemessener Frist, in der Regel mindestens 30 Kalendertage vor Durchführung, anzukündigen.

(6) Kontrollen dürfen den Geschäftsbetrieb des Auftragsverarbeiters nicht unangemessen beeinträchtigen und haben unter Berücksichtigung von Betriebs- und Geschäftsgeheimnissen sowie datenschutzrechtlichen Verpflichtungen gegenüber anderen Kunden zu erfolgen.

(7) Der Auftraggeber trägt die Kosten der von ihm veranlassten Prüfungen, soweit die Prüfung keinen vom Auftragsverarbeiter zu vertretenden Verstoß gegen datenschutzrechtliche Vorschriften nachweist.

(8) Der Auftragsverarbeiter ist berechtigt, angemessene Maßnahmen zum Schutz seiner Geschäfts- und Betriebsgeheimnisse sowie der Rechte anderer Kunden zu treffen.

§ 11 Meldung von Datenschutzverletzungen

(1) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Auftragsverarbeitung bekannt geworden ist.

(2) Die Mitteilung erfolgt unter Berücksichtigung der dem Auftragsverarbeiter zum jeweiligen Zeitpunkt verfügbaren Informationen und enthält, soweit möglich, insbesondere Angaben zu:

- a) Art der Datenschutzverletzung,
- b) betroffenen Datenkategorien,
- c) betroffenen Personengruppen,
- d) den wahrscheinlichen Folgen der Datenschutzverletzung,
- e) den bereits ergriffenen oder geplanten Maßnahmen zur Eindämmung und Behebung des Vorfalls.

(3) Soweit zum Zeitpunkt der Erstmeldung noch nicht sämtliche Informationen vorliegen, wird der Auftragsverarbeiter verfügbare Informationen schrittweise nachreichen.

(4) Der Auftragsverarbeiter unterstützt den Auftraggeber im angemessenen Umfang bei der Erfüllung etwaiger gesetzlicher Melde- und Benachrichtigungspflichten gegenüber Aufsichtsbehörden und betroffenen Personen.

(5) Die Bewertung, ob eine Datenschutzverletzung gegenüber einer Aufsichtsbehörde oder betroffenen Personen meldepflichtig ist, obliegt grundsätzlich dem Auftraggeber als Verantwortlichem.

(6) Die Meldung einer Datenschutzverletzung durch den Auftragsverarbeiter stellt kein Anerkenntnis einer Verantwortlichkeit oder Haftung dar.

§ 12 Löschung und Rückgabe von Daten

(1) Nach Beendigung der Auftragsverarbeitung stellt der Auftragsverarbeiter dem Auftraggeber auf dessen Anforderung die im Rahmen der vertragsgemäßen Nutzung der Plattform verarbeiteten personenbezogenen Daten in einem von dem Auftragsverarbeiter unterstützten Standardformat zur Verfügung.

(2) Der Auftraggeber kann die Bereitstellung der Daten innerhalb von 30 Kalendertagen nach Beendigung des Vertragsverhältnisses verlangen.

(3) Weitergehende Migrations-, Konvertierungs-, Aufbereitungs-, Beratungs- oder Unterstützungsleistungen sind nicht Bestandteil dieser Vereinbarung und bedürfen einer gesonderten Vereinbarung.

(4) Nach Ablauf der Bereitstellungsfrist gemäß Absatz 2 ist der Auftragsverarbeiter berechtigt, die personenbezogenen Daten zu löschen oder zu anonymisieren, soweit keine gesetzlichen Aufbewahrungspflichten, behördlichen Anordnungen oder sonstigen gesetzlichen Verpflichtungen einer Löschung entgegenstehen.

(5) Soweit gesetzliche Aufbewahrungspflichten bestehen, wird der Auftragsverarbeiter die betreffenden Daten bis zum Ablauf der jeweiligen Aufbewahrungsfrist aufbewahren und anschließend löschen.

(6) Von der Löschung ausgenommen sind Daten, die sich in Sicherungskopien (Backups) befinden, soweit deren gesonderte Löschung nur mit unverhältnismäßigem technischem Aufwand möglich wäre. Solche Daten werden ausschließlich zu Sicherheitszwecken vorgehalten und nach Ablauf der jeweiligen Backup-Aufbewahrungsfristen gelöscht.

(7) Der Auftragsverarbeiter wird dem Auftraggeber auf Anforderung die Durchführung der Löschung oder Anonymisierung in angemessener Weise bestätigen.

(8) Gesetzliche Aufbewahrungs-, Nachweis- und Dokumentationspflichten bleiben unberührt.

§ 13 Schlussbestimmungen

(1) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag.

(2) Im Falle von Widersprüchen zwischen dieser Vereinbarung und sonstigen vertraglichen Vereinbarungen der Parteien gehen die Regelungen dieser Vereinbarung hinsichtlich der Auftragsverarbeitung personenbezogener Daten vor.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist.

(4) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam, undurchführbar oder nichtig sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(5) Die Parteien verpflichten sich, eine unwirksame oder undurchführbare Bestimmung durch eine solche Regelung zu ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck der ursprünglichen Bestimmung möglichst nahekommt.

(6) Soweit in dieser Vereinbarung nichts Abweichendes geregelt ist, gelten die Bestimmungen des zwischen den Parteien geschlossenen Softwarenutzungsvertrages einschließlich seiner Anlagen.

(7) Diese Vereinbarung tritt mit Inkrafttreten des zugrunde liegenden Softwarenutzungsvertrages in Kraft und endet automatisch mit dessen Beendigung, soweit keine gesetzlichen Aufbewahrungs- oder Nachwirkungspflichten bestehen.

(8) Die folgenden Anlagen sind Bestandteil dieser Vereinbarung:

- Anlage 1 – Beschreibung der Verarbeitung
- Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)
- Anlage 3 – Unterauftragsverarbeiter

(9) Die Unterzeichnung dieser Vereinbarung kann auch mittels qualifizierter, fortgeschrittener oder sonstiger elektronischer Signatur erfolgen, soweit gesetzlich zulässig.

Düsseldorf, den 01.06.2026

Für den Kunden Name, Funktion	Für die aurixus GmbH Christian Schmid, Geschäftsführer
----------------------------------	---

Anlagen

Anlage 1 Beschreibung der Verarbeitung

Anlage 2 Technische und organisatorische Maßnahmen (TOMs)

Anlage 3 Unterauftragsverarbeiter

ANLAGE 1

BESCHREIBUNG DER VERARBEITUNG

1. Gegenstand der Verarbeitung

Der Auftragsverarbeiter stellt dem Auftraggeber die Plattform „DigitalCheckIn Education“ einschließlich der beauftragten Erweiterungsmodule, Anwendungen, Schnittstellen, Hardwarekomponenten und sonstigen vereinbarten Leistungen zur Verfügung.

Die Verarbeitung erfolgt ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen.

2. Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten kann insbesondere erfolgen zur:

- Teilnehmerverwaltung
- Benutzer- und Rollenverwaltung
- Kurs- und Maßnahmenverwaltung
- Standortverwaltung
- Anwesenheits- und Nachweisdokumentation
- Erfassung von Check-In- und Check-Out-Vorgängen
- Erfassung und Verwaltung digitaler Signaturen
- Durchführung von Authentifizierungs- und Autorisierungsvorgängen
- Erstellung von Berichten, Auswertungen und Exporten
- Durchführung von Kommunikations- und Benachrichtigungsprozessen
- Durchführung von Workflow-, Automatisierungs- und Monitoringprozessen
- Verwaltung und Überwachung freigegebener Hardwarekomponenten
- Fehleranalyse, Support und Wartung
- Durchführung von Analyse-, Automatisierungs- und KI-gestützten Funktionen, soweit diese vom Auftraggeber aktiviert wurden

3. Kategorien betroffener Personen

Von der Verarbeitung können insbesondere folgende Personengruppen betroffen sein:

- Teilnehmer
- Mitarbeiter des Auftraggebers
- Dozenten
- Referenten
- Prüfer
- Administratoren

- Ansprechpartner des Auftraggebers
- sonstige durch den Auftraggeber verwaltete Personen

4. Kategorien personenbezogener Daten

Verarbeitet werden können insbesondere:

- Vorname
- Nachname
- Benutzername
- Teilnehmernummer
- Personalnummer
- E-Mail-Adresse
- Telefonnummer
- Rollen und Berechtigungen
- Kurs- und Maßnahmenzuordnungen
- Standortzuordnungen
- Anwesenheitsdaten
- Check-In- und Check-Out-Daten
- Zeitstempel
- digitale Signaturen
- NFC-Tag- oder Kartennummern
- Kommunikationsdaten
- Audit- und Protokolldaten
- sonstige durch den Auftraggeber bereitgestellte personenbezogene Daten

5. Besondere Kategorien personenbezogener Daten

Die vertragsgemäße Nutzung der Plattform ist nicht auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO ausgelegt.

Eine Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt nur, soweit dies ausdrücklich zwischen den Parteien vereinbart wurde.

6. Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des zwischen den Parteien bestehenden Vertragsverhältnisses einschließlich der in der AVV geregelten Aufbewahrungs-, Bereitstellungs- und Löschfristen.

7. Verarbeitungsorte

Die Verarbeitung erfolgt innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR).

Zum Einsatz kommen insbesondere:

- Hetzner Online GmbH (Deutschland)
- Microsoft Azure (Germany West Central, Frankfurt am Main)

Weitere Verarbeitungsorte ergeben sich gegebenenfalls aus Anlage 3 (Unterauftragsverarbeiter).

ANLAGE 2

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMs)

1. Vertraulichkeit

1.1 Zutrittskontrolle

Der Zugang zu Systemen und Infrastrukturen wird durch geeignete organisatorische und technische Maßnahmen geschützt.

Hierzu gehören insbesondere:

- Zugangsbeschränkungen zu Betriebs- und Verwaltungsbereichen
- kontrollierter Zugang zu technischen Systemen
- Berechtigungskonzepte
- Besucherkontrollen soweit erforderlich

1.2 Zugangskontrolle

Der Zugriff auf Systeme erfolgt ausschließlich für autorisierte Personen.

Hierzu gehören insbesondere:

- Benutzerkonten
- individuelle Anmeldedaten
- Passwortschutz
- rollenbasierte Berechtigungen
- Multi-Faktor-Authentifizierung (soweit eingesetzt)
- Single-Sign-On-Verfahren (soweit eingesetzt)

1.3 Zugriffskontrolle

Personenbezogene Daten dürfen nur im Rahmen der jeweils erteilten Berechtigungen verarbeitet werden.

Hierzu gehören insbesondere:

- Rollen- und Berechtigungskonzepte
- Mandantentrennung
- Berechtigungsprüfungen
- regelmäßige Überprüfung von Berechtigungen

1.4 Trennungskontrolle

Daten verschiedener Kunden werden logisch voneinander getrennt verarbeitet.

Hierzu gehören insbesondere:

- Mandantenfähigkeit

- getrennte Datenhaltung innerhalb der Plattform
- rollenbasierte Zugriffsbeschränkungen

2. Integrität

2.1 Weitergabekontrolle

Personenbezogene Daten werden ausschließlich über gesicherte Kommunikationswege übertragen.

Hierzu gehören insbesondere:

- TLS-verschlüsselte Verbindungen
- HTTPS
- verschlüsselte Schnittstellenkommunikation
- Authentifizierungsmechanismen

2.2 Eingabekontrolle

Verarbeitungsvorgänge können nachvollzogen werden.

Hierzu gehören insbesondere:

- Auditprotokolle
- Änderungsprotokolle
- Benutzerzuordnungen
- Zeitstempel

3. Verfügbarkeit und Belastbarkeit

3.1 Betriebs- und Ausfallsicherheit

Es werden Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme getroffen.

Hierzu gehören insbesondere:

- Monitoring
- Systemüberwachung
- Sicherheitsupdates
- Fehlerbehebung
- Wartungsprozesse

3.2 Datensicherung

Zur Absicherung der Daten werden regelmäßige Datensicherungen durchgeführt.

Hierzu gehören insbesondere:

- tägliche Backups

- Aufbewahrung von Sicherungskopien für 30 Tage
- Wiederherstellungsverfahren
- regelmäßige Überprüfung der Datensicherung

3.3 Wiederherstellbarkeit

Für den Fall technischer Störungen bestehen Verfahren zur Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten.

4. Belastbarkeit und Sicherheitsmanagement

4.1 Schwachstellenmanagement

Sicherheitsrelevante Updates und Fehlerbehebungen werden angemessen bewertet und umgesetzt.

Hierzu gehören insbesondere:

- Patchmanagement
- Sicherheitsupdates
- Firmwareupdates
- Aktualisierung eingesetzter Plattformkomponenten

4.2 Sicherheitsüberwachung

Sicherheitsrelevante Ereignisse können erkannt und bewertet werden.

Hierzu gehören insbesondere:

- Systemmonitoring
- Protokollierung
- Fehler- und Ereignisanalyse

5. Verfahren zur regelmäßigen Überprüfung

5.1 Datenschutzmanagement

Der Auftragsverarbeiter überprüft regelmäßig die Wirksamkeit seiner technischen und organisatorischen Maßnahmen.

Hierzu gehören insbesondere:

- interne Prüfungen
- organisatorische Kontrollen
- Anpassung von Sicherheitsmaßnahmen
- Aktualisierung von Richtlinien

5.2 Berechtigungsmanagement

Benutzerkonten und Berechtigungen werden regelmäßig überprüft und bei Bedarf angepasst.

6. Unterstützung der Betroffenenrechte

Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung von Betroffenenrechten im Rahmen der vertraglichen und gesetzlichen Verpflichtungen.

7. Auftragskontrolle

Personenbezogene Daten werden ausschließlich im Rahmen der Weisungen des Auftraggebers verarbeitet.

Mitarbeiter werden auf Vertraulichkeit verpflichtet und hinsichtlich datenschutzrechtlicher Anforderungen sensibilisiert.

8. Hosting und Infrastruktur

Die Plattform wird auf Infrastruktur innerhalb der Europäischen Union betrieben.

Zum Einsatz können insbesondere kommen:

- Hetzner Online GmbH (Deutschland)
- Microsoft Azure (Germany West Central, Frankfurt am Main)

Die jeweils eingesetzten Unterauftragsverarbeiter ergeben sich aus Anlage 3.

9. Authentifizierung und Identitätsmanagement

Die Plattform unterstützt insbesondere:

- lokale Benutzerkonten
- Microsoft Entra ID
- SAML
- LDAP
- OpenID Connect
- Multi-Faktor-Authentifizierung

Der konkrete Umfang richtet sich nach den jeweils eingesetzten Funktionen.

10. Hardwaresicherheit

Soweit Hardwarekomponenten eingesetzt werden, werden angemessene Maßnahmen zur Absicherung der Geräte getroffen.

Hierzu können insbesondere gehören:

- Geräteverwaltung
- Remote-Konfiguration
- Sicherheitsupdates
- Firmwareupdates
- Geräteüberwachung

- Zugriffsbeschränkungen

11. Automatisierungs- und KI-Funktionen

Soweit Automatisierungs-, Analyse- oder KI-gestützte Funktionen eingesetzt werden, erfolgen deren Nutzung und Verarbeitung ausschließlich im Rahmen der vertraglich vereinbarten Leistungen.

Geeignete technische und organisatorische Maßnahmen werden berücksichtigt, um Datenschutz, Vertraulichkeit und Informationssicherheit sicherzustellen.

ANLAGE 3

UNTERAUFTRAGSVERARBEITER

Stand: 01.06.2026

Der Auftragsverarbeiter setzt zur Erbringung der vertraglich vereinbarten Leistungen folgende Unterauftragsverarbeiter ein:

Unternehmen	Leistung	Verarbeitungsort
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland	Hosting, Infrastruktur, Datenspeicherung, Datensicherung	Deutschland
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Cloud-Dienste, Authentifizierungsdienste, Integrationen, Microsoft Azure Services	Europäische Union (insbesondere Deutschland)

Hinweise

- (1) Der Auftragsverarbeiter ist berechtigt, weitere Unterauftragsverarbeiter gemäß § 8 dieser Vereinbarung einzusetzen.
- (2) Die jeweils aktuelle Liste der eingesetzten Unterauftragsverarbeiter kann vom Auftragsverarbeiter fortlaufend aktualisiert werden.
- (3) Über die Aufnahme neuer Unterauftragsverarbeiter oder wesentliche Änderungen bestehender Unterauftragsverarbeiter wird der Auftraggeber gemäß § 8 dieser Vereinbarung informiert.
- (4) Soweit künftig zusätzliche Dienste für Kommunikation, Automatisierung, Analysen, Künstliche Intelligenz, Authentifizierung, Integrationen oder sonstige Plattformfunktionen eingesetzt werden, können hierfür weitere Unterauftragsverarbeiter hinzugefügt werden.