Vertrag über die Auftragsverarbeitung personenbezogener Daten gemäß Art. 28 DSGVO
(Datenverarbeitung im Auftrag)

zwischen

[Kunde]

--- nachstehend **Auftraggeber** genannt ---

und

ORA Software GmbH
vertreten durch den Geschäftsführer
Speckweg 98a
68305 Mannheim

--- nachstehend **Auftragnehmer** genannt ---

§ 1 Allgemeines

(1) Zwischen den Parteien besteht ein Vertragsverhältnis über die Bereitstellung des Softwaresystems „Azubiheft – Das digitale Berichtsheft“. Aufgrund der Aufgabenstellung kann hierbei ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden.

(2) Der Auftragnehmer ist gegenüber seinen Mitarbeitern, Kunden und Geschäftspartnern verpflichtet, das Auftragsverhältnis mit externen Dienstleistern schriftlich zu regeln und insbesondere die Vertraulichkeit und Integrität der Daten seiner Kunden und Geschäftspartner sowie der eigenen IT-Systeme sicherzustellen.

(3) Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DSGVO als Dienstleister ausgewählt. Art. 28 DSGVO setzt eine schriftliche Auftragserteilung voraus, wenn die Verarbeitung personenbezogener Daten durch andere Stellen im Auftrag vorgenommen wird und hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i.S.d. Art. 28 DSGVO und regelt die Rechte und Pflichten der Parteien zum Datenschutz im Zusammenhang mit der Datenverarbeitung. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

(4) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

§ 2 Dauer, Laufzeit der Auftragsverarbeitung

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages. Sofern in dieser Vereinbarung

nichts anderes vereinbart ist, sind Kündigungsrechte und Anforderungen die gleichen wie im betreffenden Vertrag. Eine Verletzung dieser Vereinbarung begründet für den Auftraggeber einen wichtigen Grund, den Vertrag mit dem Auftragsnehmer außerordentlich zu kündigen.

§ 3 Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

- Bereitstellung und Hosting des Softwaresystems „Azubiheft – Das digitale Berichtsheft“
- Laufende Pflege und Wartung der Softwareplattform
- Erhebung der notwendigen persönlichen Registrierungsdaten aller „Azubiheft“ Nutzer.
- Verarbeitung und Speicherung der Berichtsheftdokumentation und der hochgeladenen Dokumente.

Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten:

Es werden Daten im Rahmen der für eine Prüfungszulassung notwendigen Berichtsheftführung erhoben, verarbeitet und genutzt, dies betrifft die Daten der beteiligten Akteure, die in der Wochendokumentation erfassten Tätigkeiten und Fertigkeiten sowie die zur Verbesserung der Dokumentation gespeicherten Dokumente. Alle prüfungsrelevanten Daten können optional durch den Nutzer der Kammer bereitgestellt werden. Die regelmäßige Art der Verarbeitung umfasst das, Erheben, Erfassen, Speichern, Abfragen, Auslesen und Übermitteln personenbezogener Daten. Der Auftragnehmer darf die vom Auftraggeber überlassenen oder für diese erhobenen Daten nicht zu eigenen Zwecken oder Zwecken Dritter, auch nicht zu Testzwecken, verarbeiten.

Art der Daten:

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten /-Kategorien

- Profildaten
  - Berufsschule, Ausbildungsbetrieb
  - Anrede, Name, Vorname, Adresse, Geburtsdatum, Telefon
  - E-Mail-Adresse, Passwort
  - Ausbildungsbezeichnung, Ausbildungszeitraum, Schule, Rahmenplan

- Berichtsheft-Daten
  - Abteilung, Lernort, Status
  - Tätigkeiten, Tätigkeitsart, Zeitdauer, Bemerkungen
  - Freigabedatum, freigebender Auszubildender
  - Abnahmedatum, kontrollierender Ausbilder

- Ausbildungsrahmenplan-Daten
  - Entwicklungsstand-Daten

- Sonstiges
  - Hochgeladene Dokumente
  - Kommentare
  - Notenspiegel

Kreis der Betroffenen:

- Beschäftigte, Mitarbeiter (Auszubildende, Ausbilder)

§ 4 Rechte und Pflichten des Auftraggebers

Der Auftraggeber hat das Recht, jederzeit Änderungen über Art, Umfang und Verfahren des in § 3 genannten Auftragsgegenstandes durchzuführen.

Änderungen können

- schriftlich
- per E-Mail

erfolgen. Ggf. mündlich erteilte Weisungen müssen umgehend schriftlich bestätigt / dokumentiert werden.
Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

Weisungsberechtigte Personen sind auf Seiten des Auftraggebers:

- Kaufmännische Ausbilderinnen und Ausbilder
- Technische Ausbilderinnen und Ausbilder
- Personalleitung

Weisungsempfänger, die berechtigt sind, Weisungen des Auftraggebers zu empfangen sind:

- Geschäftsführung
- Mitarbeiter Supportbereich

Bei einem Wechsel oder einer längerfristigen Verhinderung eines Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

(1) Änderungen über Art und Umfang der Leistungen bzw. des Vertragsverhältnisses werden schriftlich fixiert und zusammen mit der Vereinbarung so aufbewahrt, dass alle maßgeblichen Regelungen jederzeit verfügbar sind. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Ist die Rechtmäßigkeit einer Weisung zweifelhaft, ist der Auftragnehmer berechtigt, die Durchführung der Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Stehen schwere Persönlichkeitsverletzungen im Raum oder nimmt der Auftragnehmer bei weisungsgemäßen Handeln das Risiko einer strafbaren Handlung auf sich, darf er die Umsetzung der Weisung darüber hinaus aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, falls er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber ist im Rahmen der Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, die Datenweitergabe an den Auftragnehmer sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO verantwortlich.

(4) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen. Die Befugnisse der Aufsichtsbehörden – insbesondere nach Art. 58 Abs. 1 DSGVO – bleiben hiervon unberührt.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers oder eines eingesetzten Subunternehmens gegen Datenschutzvorschriften oder Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer oder das eingesetzte Subunternehmen eine Weisung des Auftraggebers nicht ausführen kann oder will, oder der Auftragnehmer oder das eingesetzte Subunternehmen Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 5 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer gestaltet seine innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft insbesondere geeignete technische und organisatorische Maßnahmen, um einen dem Risiko angemessenen Schutz der Daten des Auftraggebers zu gewährleisten (Art. 32 Abs. 1 DSGVO). Sofern personenbezogene Daten in Telearbeit und Heimarbeit verarbeitet werden, ist er verpflichtet, dies dem Auftraggeber mitzuteilen. Er trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicher gestellt sind. Die entsprechenden technischen und organisatorischen Maßnahmen ergeben sich aus (aus der Anlage zu dieser Vereinbarung, dem Sicherheitskonzept etc.). Änderungen der getroffenen Maßnahmen durch den Auftragnehmer sind nur zulässig, wenn sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber mitzuteilen und mit diesem abzustimmen. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte (Art. 28 Abs. 3 Buchst. e DSGVO) und unterstützt den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa bei erforderlichen Datenschutz-Folgenabschätzungen (Art. 28 Abs. 3 Satz 2 Buchst. f DSGVO). Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(2) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der

Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen Aufbewahrungspflichten. Nach Auftragsende sind Daten, Datenträger sowie sonstige Materialien auf Verlangen und nach Wahl des Auftraggebers entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht. Im Falle einer Inanspruchnahme des Auftraggebers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

(3) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich, spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist. Die Mitteilung hat an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

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

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

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

d) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;

(4) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(5) Der Auftragnehmer informiert den Auftraggeber unverzüglich bei Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(6) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

(7) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten personenbezogener Daten (Art. 9 DSGVO) oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll

zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

(8) Der Auftragnehmer darf, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland verarbeiten oder nutzen.

(9) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

(10) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten. Der Auftragsverarbeiter unterstützt den Verantwortlichen dabei, die Einhaltung der Sicherheit der Verarbeitung, die Datenschutzfolgeabschätzungen und die vorherigen Konsultationen im Sinne der DSGVO (Art. 32, 35 und 36) oder anderer Datenschutzgesetze durch Bereitstellung erforderlicher Informationen sicherzustellen.

Plichten der Auftragnehmers nach den Artikeln 32 – 36 der DS-GVO

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(11) Eine Weiterleitung von personenbezogenen Daten an Dritte darf nur nach vorheriger schriftlicher

Zustimmung des Auftraggebers erfolgen.

(12) Auskunftsersuchen von Dritten oder Betroffenen leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter. Auskünfte an Dritte oder Betroffene durch den Auftragnehmer bedürfen der vorherigen schriftlichen Zustimmung durch den Auftraggeber.

(13) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

§ 6 Kontrollbefugnisse

(1) Der Auftraggeber oder ein vom Auftraggeber beauftragter Dritter hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Wirkungsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftragnehmer gewährleistet das für die Durchführung der Kontrollen erforderliche Betretungsrecht, die Einsichtnahme in diesbezügliche Unterlagen, die Vorführung der im Rahmen der Auftragsdatenverarbeitung betrieblichen Abläufe und unterstützt das mit der Durchführung der Kontrolle beauftragte Personal hinsichtlich ihrer Tätigkeit. Der Auftragnehmer sorgt dafür, dass vertrauliche Informationen Dritter vor der Einsicht des zur Kontrolle beauftragten Personals geschützt ist. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um zu vermeiden, dass die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

(4) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(5) Sofern einschlägig, verpflichtet sich der Auftragnehmer, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

§ 7 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmen durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig. Vor Hinzuziehung weiterer oder Ersetzung der bisherigen Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Der Auftragnehmer darf neue Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(2) Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Die Beauftragung von Subunternehmern ist jedoch nur möglich, wenn dem Subunternehmer vertraglich Datenschutzpflichten auferlegt werden, die dem vorliegenden Vertrag vergleichbar sind.

(3) Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art.32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 DSGVO bestellt hat, sofern die Voraussetzungen für eine Bestellung vorliegen.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Subunternehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(5) Die Beauftragung des Subunternehmens muss schriftlich erfolgen. Der Auftraggeber ist berechtigt, beim Auftragnehmer Einsicht in dessen Verträge mit Subunternehmern zu nehmen und vom Auftragnehmer die Übersendung einer Kopie dieser Verträge zu verlangen.

(6) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(7) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (§ 6 dieses Vertrages) des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort Kontrollen durch den Auftraggeber oder einen beauftragten Dritten zu dulden hat.

(8) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

(9) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

(10) Die Erbringung der Datenverarbeitung des Unterauftragsverarbeiters findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt.

§ 8 Datengeheimnis

(1) Zur Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit.b, 29, 32 Abs. 4 setzt der Auftragnehmer bei der Durchführung der Arbeiten nur Beschäftigte ein, die vor ihrem erstmaligen Tätigwerden auf die Vertraulichkeit schriftlich verpflichtet und zuvor mir den für die relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

Der Auftragsverarbeiter verpflichtet sich darüber hinaus, alle nicht allgemein bekannten Angelegenheiten und insbesondere die Geschäfts-, und Betriebsgeheimnisse des Auftraggebers unbefristet streng vertraulich zu behandeln. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln.

Der Auftragsverarbeiter wird es unterlassen personenbezogene Daten des Verantwortlichen einem Dritten offen zu legen, außer wenn dies in Übereinstimmung mit dieser Vereinbarung vereinbart wurde, der Verantwortliche die Offenlegung ausdrücklich verlangt oder der Auftragsverarbeiter nach anwendbarem Recht zur Offenlegung verpflichtet ist.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese zur Vertraulichkeit verpflichtet wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(3) Die Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung des Vertragsverhältnisses fort.

§ 9 Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.

§ 10 Haftung und Schadensersatz

(1) Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

§ 11 Beendigung

(1) Nach Beendigung des Vertrages oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Die Datenträger des Auftragnehmers sind dabei so zu löschen, dass eine Wiederherstellung oder Rekonstruktion der Daten nicht möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Die Löschung bzw. Vernichtung wird dem Auftraggeber mit Datumsangabe unverzüglich schriftlich bestätigt.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

§ 12 Berichtigung, Löschung und Herausgabe

(1) Der Auftragnehmer wird die personenbezogenen Daten nur so lange aufbewahren, wie vom Auftraggeber angewiesen. Sofern keine konkrete Weisung vorliegt, werden die personenbezogenen Daten vor der Vernichtung nur so lange aufbewahrt, wie dies zur Durchführung der jeweiligen Auftragsverarbeitung unter diesem Vertrag notwendig ist.

(2) Der Auftragnehmer trifft die erforderlichen Vorkehrungen, um eine Berichtigung, Löschung und Sperrung der personenbezogenen Daten aufgrund gesetzlicher Anforderungen, auf Verlangen der Aufsichtsbehörde sowie auf Weisung des Auftraggebers vornehmen zu können.

(3) Auf Verlangen des Auftraggebers sowie nach Beendigung dieses Vertrages wird der Auftragnehmer sämtliche personenbezogenen Daten, überlassene Datenträger und Unterlagen, die im Zusammenhang mit dieser Auftragsverarbeitung stehen und personenbezogene Daten des Auftraggebers enthalten, sowie etwaige Kopien davon unverzüglich, spätestens jedoch binnen 14 Tagen nach Aufforderung und Weisung des Auftraggebers bzw. Beendigung der Auftragsverarbeitung, an den Auftraggeber zurückgeben oder unter Einhaltung einschlägiger datenschutzrechtlicher Bestimmungen löschen bzw. vernichten.

(4) Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer standardmäßig; nur in besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe. Auf Anforderung weist der Auftragnehmer dem Auftraggeber die datenschutzkonforme Vernichtung des Materials nach.

§ 13 Schlussbestimmungen

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn die Daten des Auftraggebers durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter beim Auftragnehmer gefährdet werden. Der Auftragnehmer informiert in diesem Fall alle Beteiligten unverzüglich darüber, dass das Eigentum an den Daten ausschließlich beim Auftraggeber liegt.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweises darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

Änderungen und Ergänzungen dieses Vertrages bedürfen einer schriftlichen Vereinbarung. Im Falle eines Widerspruchs zwischen dem Hauptvertrag und diesem Vertrag zur Auftragsverarbeitung geht dieser Vertrag vor, soweit die Regelung dieses Vertrags die Verarbeitung personenbezogener Daten betrifft.
Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit dieses Vertrags im Übrigen nicht.

Dieser Vertrag umfasst 11 Seiten und beinhaltet die Anlage: „*Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO.pdf*“.

Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO					
ORA Software GmbH Speckweg 98a 68308 Mannheim					**ANLAGE 1**
Stand vom:	Version	Zugehöriges Verfahren:	Bearbeitet:	Freigabe:	
	1	Azubiheft - Digitales Berichtsheft			

Gem. Art 32 Abs. 1 Datenschutzgrundverordnung (DSGVO) haben der Verantwortliche (Auftraggeber) und der Auftragsdatenverarbeiter (Auftragnehmer) geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen unter anderem folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

1. Grundinformationen

Angaben zur Hardware (Server und Endgeräte): **DELL Poweredge Server**
Serverstandort: Frankfurt im Rechenzentrum der Firma „First Colo GmbH“
Angaben zur Software (Betriebssystem(e) und Anwendungen): **Server 2019**
Angaben zur Datenspeicherung (zentral, lokal, Verschlüsselung, Downloadmöglichkeit, Speicherort usw.) **Zentral, Verschlüsselt**
Angaben zur Vernetzung (LAN / Intranet, Internet, geschlossener Benutzerkreis usw.) **Die Server sind mit 1Gbit Download und 1Gbit Upload an das Internet angeschlossen.**

2. Maßnahmen zur Pseudonymisierung und Verschlüsselung

Maßnahmen, die geeignet sind, sicherzustellen dass Informationen nur einem bestimmten Empfängerkreis zugänglich sind.

Maßnahme	Erläuterung
Passwortverschlüsselung	Die Passwörter aller Benutzer-Accounts werden ausschließlich als Hash-Werte gespeichert.

3. Maßnahmen zur Gewährleistung der Vertraulichkeit

3.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahme	Erläuterung
Zutrittskontrollsystem	Der Zutritt zu den relevanten Technikräumen wird über Zutrittskontrollen bzw. -regelungen abgesichert. Hierzu existieren entsprechende organisatorische Anweisungen und elektronische Zutrittskontrollsysteme.
Ausführung Serverraum	Der Serverraum ist fensterlos.
Überwachung	Es erfolgt eine 24-Stunden-Bewachung durch einen Schließdienst.

3.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahme	Erläuterung
Zugangs- und Berechtigungsmanagement	Der Zugang zu den betroffenen Softwaresystemen wird generell nur über personalisierte Logins gewährt.
Administratoren	Die Anzahl der Personen mit administrativen Zugriffsmöglichkeiten auf Daten des Auftraggebers ist stets auf ein erforderliches Minimum reduziert.
Passwortrichtlinien	Die Zugangsberechtigungen sind mit zeitgemäßem Passwortschutz abgesichert (Passwortregeln, u.a. Anzeige der Passwortqualität beim Festlegen eines neuen Passworts).
Netzwerkabsicherung	Der Betrieb der Server erfolgt in einer nach dem Stand der Technik abgesicherten Umgebung mit Firewall.
Verschlüsselung von Passwörtern	Die Passwörter aller Benutzer-Accounts werden ausschließlich als Hash-Werte gespeichert.
Einsatz von Anti-Viren-Software	Es kommt Antiviren Software zum Einsatz.
Protokollierung Zugang	Der Zugang zu Datenverarbeitungssystemen wird protokolliert.
Sperrung / Entzug von Berechtigungen	Anmelderechte ausgeschiedener Mitarbeiter werden sofort nach Beendigung des Arbeitsvertrages entzogen.

3.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahme	Erläuterung
Berechtigungsmanagement	Spezifische administrative Rechte werden durch ein dokumentiertes Rollenkonzept nachvollziehbar den jeweiligen Nutzern (Administratoren) zugeordnet.
Administration	Zugriff auf Daten des Auftraggebers haben nur Personen, die mit der Sicherstellung des ordnungsgemäßen und fehlerfreien Betriebs des Systems beauftragt sind.
Datenträgerentsorgung	Nicht mehr benötigte Datenträger werden durch Dienstleister vernichtet.
Protokollierung	Zugriffe auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten werden protokolliert.
Datenträgerlöschung	Datenträger werden vor der Wiederverwendung physisch gelöscht.
Datenträgervernichtung	Die Vernichtung von Datenträgern erfolgt gemäß der DIN 66399 (vormals 32757)
Anzahl Administratoren	Die Anzahl von Administratoren ist auf das Notwendigste reduziert.
Sichere Aufbewahrung von Datenträgern	Datenträger werden sicher aufbewahrt.
Trennung Test- / Produktivsysteme	Es existieren getrennte Test- und Produktivsysteme.

3.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahme	Erläuterung
Prüfung Vertragsausführung	Es erfolgen regelmäßige Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung.
Anpassung von Regelungen	Notwendige Anpassungen von Regelungen und Maßnahmen zur Durchführung des Auftrags werden vorgenommen.
Auftragserteilung	Es besteht eine formalisierte Auftragserteilung.
Datenschutzbeauftragter	Der Auftragnehmer hat einen fachkundigen externen Datenschutzbeauftragten bestellt. Kontakt des Datenschutzbeauftragten: Datenschutz- & IT-Security Management Beratung, Dierk Kallendorf, Feldstrasse 21 b, 64839 Münster

3.5 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahme	Erläuterung
Mandantenfähigkeit	Das Anwendungssystem Azubiheft ist umfassend mandantenfähig.

4. Maßnahmen zur Gewährleistung der Integrität

4.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahme	Erläuterung
Datenübertragung physisch	Die Datenübertragung erfolgt nicht auf physischen Datenträgern.
Verschlüsselter Datenaustausch in Web-Anwendungen	Die Datenübertragung im Internet erfolgt über verschlüsseltes https.
Datenübertragung Netzwerk	Datenübertragung im Zusammenhang mit Backups oder sonstigen Administrativen Tätigkeiten (beim Auftragnehmer) finden generell über ein getunneltes VPN (Virtual Privat Network) statt.
Datenübermittlung an Dritte	Eine Datenübermittlung personenbezogener Daten an Dritte durch den Auftragnehmer selbst erfolgt nicht.

4.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahme	Erläuterung
Zuordnung Eingaben	Alle Dateneingaben in das Anwendungssystem Azubiheft werden dem entsprechenden Benutzer zugeordnet und sind daher nachvollziehbar.
Protokollierung Änderungsmanagement	Aussagen über die durchgeführten Änderungen an den Server-Systemen (Gründe, Zeitpunkt u. Ergebnis) sind schriftlich hinterlegt und können im Bedarfsfall ausgewertet werden.

5. Maßnahmen zur Gewährleistung der Verfügbarkeit

5.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahme	Erläuterung
Datensicherung	Die Datensicherung erfolgt mittels eines Backup-Verfahren (siehe Vertrag)
Unterbrechungsfreie Stromversorgung	Eine Unterbrechungsfreie Stromversorgung (USV) ist gegeben.
Netzwerksicherheit	Eine Firewall ist vorhanden.
Notfallmanagement	Ein Notfallplan für Systemausfälle ist vorhanden.
Feuer- und Rauchmeldeanlagen	Es existieren Feuer- und Rauchmeldeanlagen.
Klimatisierung	Es sind Klimaanlagen vorhanden.
Physikalische Einflüsse	Temperatur und Luftfeuchtigkeitssensoren vorhanden.

5.2 Maßnahmen zur raschen Wiederherstellung bei physischem / technischem Zwischenfall

Maßnahmen, die gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Maßnahme	Erläuterung
Serverredundanz	Die Hardware für „Azubiheft“ ist redundant ausgelegt. Fällt ein Server physisch aus, können die Daten in einer kurzen Zeit auf einem zweiten Server wiederhergestellt werden.

6. Maßnahmen zur Gewährleistung der Belastbarkeit

6.1 Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Maßnahmen, die geeignet sind, um die Belastbarkeit der Systeme zu gewährleisten.

Maßnahme	Erläuterung
Sicherheitssoftware	Einsatz von Virenscannern, Firewalls
Serverredundanz	Die Systeme für „Azubiheft“ sind redundant ausgelegt.
Zutrittskontrolle	Zutrittskontrolle im Rechenzentrum
Performance Messung	Die Verarbeitung der WEB-Anfragen wird dauerhaft überwacht. Fällt die Dauer der Verarbeitung für WEB-Anfragen dauerhaft unter einen bestimmten Zeitwert, so werden entsprechende Maßnahmen getroffen um die Leistung wieder zu erhöhen.
Monitoring	Monitoring aller relevanten Infrastrukturkomponenten (Strom, Klimatisierung, Netzwerk, Sicherheit, Backup)
USV	Einsatz von Systemen zur unterbrechungsfreien Stromversorgung (USV)

7. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

7.1 Kontrollverfahren

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Maßnahme	Erläuterung
Regelmäßige Updates	Auf den Servern werden wöchentlich Updates installiert.
Aktuelles Betriebssystem	Es wird immer ein Betriebssystem eingesetzt, welches durch den Hersteller durch Updates und Patches unterstützt wird.
Aktueller Virenschutz	Virenschutz Pattern werden regelmäßig aktualisiert.
Penetrationstest	Umfassender Sicherheitstest der WEB-Anwendung durch ein IT-Sicherheitsunternehmen

8. Organisationskontrolle

Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet ist, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Maßnahme	Erläuterung
Maßnahmen	Siehe Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle
Datenschutzbeauftragter	Externer Datenschutzbeauftragter wird in regelmäßigen Abständen bestellt.