EST.2025

BeAFox

WISSEN, GELD, FREIHEIT

AVV

§ 1. Präambel

Dieser Auftragsverarbeitungsvertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Sinne von Art. 28 DSGVO.

Der Verantwortliche nutzt die Lernplattform „BeAFox“, bestehend aus der mobilen App (iOS/Android), dem Backend, dem Datenbank-Hosting, dem webbasierten Dashboard sowie begleitenden Workshops. Der Auftragsverarbeiter verarbeitet im Rahmen dieses Einsatzes personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen.

Diese Vereinbarung ergänzt den zwischen den Parteien geschlossenen Lizenz- und Nutzungsvertrag über die BeAFox-Plattform und regelt die hierfür erforderliche Verarbeitung personenbezogener Daten sowie die hierzu getroffenen technischen und organisatorischen Maßnahmen.

§ 2. Gegenstand und Dauer der Verarbeitung

1. Gegenstand dieses Auftragsverarbeitungsvertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Zusammenhang mit der Nutzung der digitalen Lernplattform „BeAFox“ durch den Verantwortlichen. Die Verarbeitung umfasst sämtliche Funktionen und Dienstleistungen, die für den technischen, organisatorischen und pädagogischen Betrieb der Plattform erforderlich sind. Dies beinhaltet insbesondere den Betrieb der mobilen Applikation (iOS/Android), des webbasierten Dashboards, der Backend-Infrastruktur, der Datenbank sowie ergänzender Services wie Supportleistungen, Workshops und laufende Weiterentwicklungen.
   Im Rahmen des Betriebs der mobilen App verarbeitet der Auftragsverarbeiter personenbezogene Daten, die für die Bereitstellung von Lernmodulen, Quizfunktionen, Fortschrittsmessungen, Gamification-Elementen und Nutzerkonten erforderlich sind. Dazu gehört auch die Verarbeitung von Aktivitäts- und Nutzungsdaten, die dem Zweck dienen, Lernstände abzubilden, Lernerfolge sichtbar zu machen oder didaktische Elemente zu personalisieren.
   Zur Unterstützung von Lehrkräften, Ausbildern oder Administratoren betreibt der Auftragsverarbeiter ein webbasiertes Dashboard, das die Verwaltung von Nutzerdaten, die Einsicht in Lernfortschritte sowie die Lizenz- und Gruppenverwaltung ermöglicht. Im Rahmen dieser Nutzung verarbeitet der Auftragsverarbeiter sowohl personenbezogene als auch aggregierte oder pseudonymisierte Daten, soweit dies zur Erfüllung der pädagogischen oder organisatorischen Aufgaben des Verantwortlichen notwendig ist.

Ferner umfasst der Auftrag das Hosting der Plattform, den Betrieb aller technischen Systeme sowie die Speicherung personenbezogener Daten innerhalb der Europäischen Union. Die Daten werden in einer MongoDB-Datenbank in der Region Frankfurt verarbeitet; die Backend- und Serverinfrastruktur wird über Render in der gleichen Region betrieben. Bestandteil der Verarbeitung sind auch Login-Mechanismen, API-Schnittstellen, Sicherheitsmaßnahmen und sämtliche weiteren technischen Prozesse, die für die Funktionsfähigkeit der Plattform erforderlich sind.
Darüber hinaus erbringt der Auftragsverarbeiter Support- und Serviceleistungen, etwa die Bearbeitung technischer Anfragen, die Durchführung von Fehleranalysen, die Bereitstellung von Dokumentationen sowie das Management sicherheitsrelevanter Ereignisse. Die Verarbeitung personenbezogener Daten kann in diesem Zusammenhang erforderlich sein, jedoch nur in dem Umfang, wie es für die Bearbeitung der Supportfälle notwendig ist.
Im Rahmen von Workshops, Onboarding-Prozessen und pädagogischen Begleitmaßnahmen kann der Auftragsverarbeiter organisatorische Informationen wie Teilnehmerlisten oder Kontaktdaten verarbeiten, sofern dies zur Durchführung der vereinbarten Leistungen erforderlich ist. Auch die Weiterentwicklung der App, die Bereitstellung neuer Inhalte, technische Wartungen sowie planmäßige Updates fallen in den Gegenstandsbereich der Verarbeitung, soweit sie mit personenbezogenen Daten in Berührung kommen.

2. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen gemäß Art. 28 Abs. 3 lit. a DSGVO. Der Auftragsverarbeiter ist nicht berechtigt, personenbezogene Daten eigenständig zu verändern, zu erweitern, für eigene Zwecke zu nutzen oder an Dritte weiterzugeben, es sei denn, dies ist zur Erfüllung des Auftrags zwingend erforderlich und wurde vorab durch den Verantwortlichen ausdrücklich genehmigt. Eine Verarbeitung für eigene oder fremde Zwecke ist ausgeschlossen.

3. Die Dauer dieses Auftragsverarbeitungsvertrags entspricht der Laufzeit des zwischen den Parteien bestehenden Lizenz- und Nutzungsvertrags über die BeAFox-Plattform. Mit Beendigung des Hauptvertrags endet auch dieser Auftragsverarbeitungsvertrag automatisch, ohne dass es einer gesonderten Kündigung bedarf.

   Nach Vertragsende werden alle personenbezogenen Daten innerhalb einer Frist von 30 Tagen entweder auf Weisung des Verantwortlichen in einem gängigen

maschinenlesbaren Format (insbesondere CSV oder JSON) zurückgegeben oder gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Backups, die personenbezogene Daten enthalten könnten, werden im Rahmen der regulären Backup-Zyklen automatisch überschrieben und nach Ablauf des Löschzyklus ebenfalls gelöscht.
Die Verpflichtungen zur Wahrung der Vertraulichkeit sowie sämtliche datenschutzrechtlichen Pflichten bestehen über die Beendigung dieses Vertrags hinaus fort.

§ 3. Art und Zweck der Verarbeitung

1. Die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter umfasst sämtliche automatisierten und teilautomatisierten Vorgänge, die zur Nutzung der Lernplattform „BeAFox“ erforderlich sind. Dies schließt insbesondere die Erhebung, Speicherung, Organisation, Anpassung, Auswertung, Übermittlung, Bereitstellung, Einschränkung, Löschung und Sicherung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DSGVO ein. Die Verarbeitung erfolgt ausschließlich innerhalb der technischen Infrastruktur der Plattform und dient der Erfüllung der vertraglich vereinbarten Leistungen.

2. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zu den im Folgenden beschriebenen, eindeutig bestimmten und legitimen Zwecken. Zentraler Zweck der Verarbeitung ist die Bereitstellung und Nutzung der mobilen App „BeAFox“. Hierzu zählt die Verwaltung von Nutzerkonten, die Authentifizierung sowie die Verknüpfung von Nutzern mit Lernmodulen, Quizfunktionen und Gamification-Elementen. Die Plattform speichert und verarbeitet individuelle Lernfortschritte, Aktivitätsdaten und Ergebnisse, um personalisierte Lerninhalte bereitzustellen und Lernprozesse sichtbar zu machen. Dies umfasst unter anderem absolvierte Module, Testergebnisse, erworbene Erfahrungspunkte sowie die dokumentierte Nutzung einzelner Funktionen.
Die Plattform dient zudem der pädagogischen Unterstützung. Der Auftragsverarbeiter verarbeitet hierzu Lernstands- und Aktivitätsdaten, um verantwortlichen Lehrkräften, Ausbildern oder Administratoren eine pädagogisch sinnvolle Übersicht über den Fortschritt der ihnen zugeordneten Lernenden zu ermöglichen. Diese Daten können aggregiert oder pseudonymisiert dargestellt werden, wobei eine Profilbildung zu Zwecken außerhalb der Lernstandsvisualisierung ausdrücklich ausgeschlossen ist.
Weiterhin erfolgt eine Verarbeitung personenbezogener Daten zur Nutzung des Dashboards durch pädagogische und organisatorische Rollen. Dies umfasst die

Verwaltung von Nutzergruppen, Kursen, Klassen und Lizenzen sowie die Einsicht in Lernstände, um Lernprozesse organisieren und begleiten zu können. Die Einsicht erfolgt stets im Rahmen der zugewiesenen Rolle und ausschließlich zu pädagogischen Zwecken.
Für den technischen Betrieb der Plattform verarbeitet der Auftragsverarbeiter Daten, die notwendig sind, um die Funktionsfähigkeit, Stabilität und Sicherheit der Systeme zu gewährleisten. Dies umfasst den Betrieb der Backend-Systeme, Datenbanken und Server, die Speicherung der Daten in der EU (Region Frankfurt), die Durchführung technischer Wartungsarbeiten sowie die Überwachung sicherheitsrelevanter Ereignisse. Auch die Protokollierung technischer Prozesse zur Fehleranalyse, Systemoptimierung oder Missbrauchserkennung erfolgt ausschließlich im notwendigen Umfang und unter Beachtung der Grundsätze der Datenminimierung.
Im Rahmen des Supports kann der Auftragsverarbeiter personenbezogene Daten verarbeiten, soweit dies zur Bearbeitung technischer Anfragen, zur Fehlersuche oder zur Kommunikation mit den zuständigen Ansprechpartnern erforderlich ist. Die Verarbeitung erfolgt dabei stets zweckgebunden und in enger Abstimmung mit dem Verantwortlichen.
Darüber hinaus kann der Auftragsverarbeiter zur Durchführung von Workshops, Onboardings und pädagogischen Schulungsmaßnahmen organisatorische Informationen wie Teilnehmerdaten verarbeiten, sofern dies zur Durchführung der vereinbarten Leistungen erforderlich ist. Eine Verarbeitung zu darüber hinausgehenden Zwecken findet nicht statt.
Zur Qualitätssicherung und Weiterentwicklung der Plattform kann der Auftragsverarbeiter anonymisierte oder pseudonymisierte Daten auswerten, um technische Abläufe zu verbessern, die Benutzerfreundlichkeit zu erhöhen oder neue Lerninhalte zu entwickeln. Personenbeziehbare Daten werden hierfür nicht verwendet.

3. Eine Verarbeitung personenbezogener Daten zu unzulässigen oder nicht vereinbarten Zwecken ist ausgeschlossen. Insbesondere ist ausgeschlossen, dass Daten zu Werbezwecken, zur Profilerstellung außerhalb des Lernkontextes, zur Weitergabe an unbefugte Dritte oder zur kommerziellen Analyse genutzt werden. Der Auftragsverarbeiter trifft geeignete Maßnahmen, um sicherzustellen, dass keine Entscheidungen getroffen werden, die gegenüber den Betroffenen eine rechtliche Wirkung entfalten oder diese erheblich beeinträchtigen würden. Eine automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO findet nicht statt.

4. Die Verarbeitung erfolgt ausschließlich zur Erfüllung des Lizenz- und Nutzungsvertrags und unterliegt dem Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 lit. b DSGVO. Eine Erweiterung oder Änderung der Verarbeitungszwecke ist nur zulässig, wenn der Verantwortliche dies zuvor ausdrücklich in Textform angewiesen hat und die geänderte Verarbeitung datenschutzrechtlich zulässig ist. Ohne eine solche Weisung ist der Auftragsverarbeiter nicht befugt, personenbezogene Daten für andere oder eigene Zwecke zu verwenden.

4. Kategorien personenbezogener Daten

1. Der Auftragsverarbeiter verarbeitet im Auftrag des Verantwortlichen ausschließlich diejenigen personenbezogenen Daten, die für den Betrieb, die Nutzung und die pädagogische Funktionalität der BeAFox-Plattform erforderlich sind. Die Verarbeitung beschränkt sich auf solche Daten, die zur Identifikation der Nutzer:innen, zur Unterstützung der Lernprozesse, zur Dokumentation des Lernfortschritts, zur technischen Bereitstellung der Plattform sowie zur Kommunikation im Rahmen von Support- oder Organisationsprozessen notwendig sind. Eine Verarbeitung darüber hinausgehender oder für die Bildungszwecke nicht relevanter Informationen findet nicht statt.

2. Zu den verarbeiteten Kategorien gehören zunächst Stammdaten der Nutzer:innen, die der Identifikation und der Zuordnung von Benutzerkonten dienen. Dazu können Vor- und Nachnamen gehören, sofern der Verantwortliche diese Form der Kontoführung einsetzt oder sie für organisatorische Zwecke erforderlich sind. Die Plattform ermöglicht jedoch auch eine vollständig pseudonymisierte Nutzung über Aliasnamen oder Initialen, insbesondere für jüngere Schüler:innen. Unabhängig davon ist die Angabe eines Benutzernamens erforderlich, um ein Nutzerkonto anlegen zu können. Zusätzlich können E-Mail-Adressen verarbeitet werden, sofern dies durch die gewählte Kontoart vorgesehen ist oder vom Verantwortlichen zur Benutzerverwaltung genutzt wird. Weiterhin werden Informationen zur Gruppenzugehörigkeit, wie Klassen, Kurse oder Ausbildungsjahrgänge, sowie die jeweilige Rolle innerhalb der Plattform (z. B. Lernende, Lehrkräfte, Administratoren) verarbeitet.

3. Darüber hinaus verarbeitet der Auftragsverarbeiter Nutzungs- und Lerndaten, die während der aktiven Nutzung der Plattform entstehen und notwendig sind, um Lernfortschritte sichtbar zu machen, Lernprozesse zu steuern und die pädagogische Zielsetzung zu erfüllen. Hierzu gehören Informationen über absolvierte Module, Testergebnisse, Quizantworten, erzielte Punktwerte,

gesammelte Erfahrungspunkte, erworbene Badges sowie der individuelle Fortschrittsstatus pro Lerneinheit. Auch zeitliche Informationen wie Start- und Abschlusszeitpunkte oder Unterbrechungen der Lerneinheiten werden erfasst. Diese Daten dienen ausschließlich der Lernstandsermittlung und werden nicht zu Profiling- oder Marketingzwecken verarbeitet.

4. Zur Gewährleistung eines stabilen und sicheren technischen Betriebs werden zusätzlich technische System- und Protokolldaten erhoben. Dazu zählen Informationen wie der verwendete Gerätetyp, Betriebssystemversionen, App-Versionen sowie technische Verbindungsdaten, die in pseudonymisierter oder anonymisierter Form verarbeitet werden. Auch Serverlogs, Absturzberichte und Login- oder Logout-Zeitpunkte können verarbeitet werden. Diese Daten dienen ausschließlich der Stabilität, Funktionsüberwachung und technischen Fehleranalyse der Plattform und werden nicht mit pädagogischen Informationen verknüpft.

5. Für pädagogische und organisatorische Aufgaben werden Daten von Lehrkräften, Ausbilder:innen und Administrator:innen verarbeitet. Diese umfassen in der Regel Namen, dienstliche E-Mail-Adressen, organisatorische Zugehörigkeiten wie Standort, Fachbereich oder Abteilung sowie die jeweils zugewiesenen Berechtigungen im Dashboard. Die Verarbeitung beschränkt sich auf diejenigen Daten, die zur Ausübung ihrer administrativen oder pädagogischen Aufgaben erforderlich sind.

6. Im Rahmen von Support- oder Onboarding-Prozessen kann der Auftragsverarbeiter Kommunikationsdaten verarbeiten. Dazu gehören Inhalte von Supportanfragen, technische Screenshots, Fehlermeldungen oder Metadaten der Kommunikation, wenn sie für die Bearbeitung eines technischen Problems notwendig sind. Bei Workshops oder Schulungen können auch Daten wie Teilnehmerlisten oder Ansprechpartner für organisatorische Zwecke verarbeitet werden. Solche Daten werden nur so lange gespeichert, wie es für die Bearbeitung der jeweiligen Anfrage erforderlich ist.

7. Zum Schutz der betroffenen Personen und insbesondere minderjähriger Lernender werden bestimmte besonders sensible Daten ausdrücklich nicht verarbeitet. Der Auftragsverarbeiter erhebt und verarbeitet keine Gesundheitsdaten, biometrischen Merkmale, Standortdaten wie GPS-Informationen, Zahlungsdaten, Informationen zu religiösen oder politischen Überzeugungen oder andere

besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO. Ebenso findet keine Verarbeitung statt, die auf Profilbildung außerhalb des Lernkontexts abzielt, und es erfolgt keine werbliche Nutzung der Daten oder Weitergabe an Dritte außerhalb der vertraglich genehmigten Subunternehmer.

8. Die im Rahmen der Plattform verarbeiteten Daten sind grundsätzlich als Daten des normalen Risikobereichs einzuordnen. Aufgrund der Tatsache, dass ein erheblicher Teil der Nutzer:innen minderjährige Lernende sein können, werden sie jedoch mit erhöhten Schutzanforderungen behandelt. Dies umfasst insbesondere strenge Grundsätze der Datenminimierung, pseudonymisierte Darstellungen, wenn möglich, sowie die konsequente Beschränkung auf pädagogisch notwendige Informationen. Öffentliche Darstellungen personenbezogener Daten oder unkontrollierte Zugriffe durch unbefugte Personen werden durch technische und organisatorische Maßnahmen ausgeschlossen.

5. Kategorien betroffener Personen

1. Der Auftragsverarbeiter verarbeitet im Rahmen der Nutzung der BeAFox-Plattform personenbezogene Daten verschiedener Kategorien betroffener Personen. Die Zugehörigkeit zu den einzelnen Gruppen ergibt sich aus der Art der Nutzung, den pädagogischen und organisatorischen Aufgaben des Verantwortlichen sowie den technischen Notwendigkeiten der Plattform. Die Verarbeitung erfolgt stets zweckgebunden, beschränkt auf das Erforderliche und unter Berücksichtigung der besonderen Schutzbedürftigkeit einzelner Personengruppen – insbesondere minderjähriger Lernender.

2. Eine zentrale Betroffenengruppe sind die Nutzer:innen der mobilen App, zu denen Schüler:innen, Auszubildende und Studierende gehören können. Schüler:innen nutzen die Plattform im Rahmen schulischer Bildungsprozesse, etwa im Unterricht oder in pädagogisch begleiteten Lernphasen. Da es sich dabei häufig um Minderjährige handelt, unterliegt die Verarbeitung besonders strengen datenschutzrechtlichen Anforderungen. Ihre Daten werden ausschließlich zur Lernstandsabbildung, zur Bereitstellung didaktischer Inhalte und zur Ermöglichung eines personalisierten Lernfortschritts verarbeitet. Auszubildende nutzen die Plattform überwiegend für berufliche oder private Finanzbildungszwecke, während Studierende die App zur Erweiterung ihrer Finanzkompetenzen im akademischen oder praxisnahen Kontext verwenden.
   Für alle Lernenden gilt: Die Verarbeitung erfolgt ausschließlich im Kontext der Lernprozesse, und es werden keine Daten zu Werbe-, Tracking- oder

Profilingzwecken außerhalb der Bildungsfunktion erhoben.

3. Darüber hinaus verarbeitet der Auftragsverarbeiter personenbezogene Daten von Personen, die beim Verantwortlichen pädagogische oder organisatorische Aufgaben wahrnehmen. Hierzu gehören Lehrkräfte, pädagogische Mitarbeitende und Ausbilder:innen, die das Dashboard nutzen, um Lernfortschritte einzusehen, Lernende zu begleiten und organisatorische Aufgaben wie die Verwaltung von Gruppen, Kursen oder Klassen durchzuführen. Auch Mitarbeitende der Schulverwaltung oder betriebliche Verwaltungsangestellte können betroffen sein, sofern sie organisatorische oder datenschutzbezogene Aufgaben ausüben. Die Verarbeitung ihrer Daten beschränkt sich auf dienstliche Informationen, die für die Erfüllung ihrer Aufgaben im Rahmen des Einsatzes der Plattform erforderlich sind.

4. Eine weitere Betroffenengruppe umfasst administrierende Personen des Verantwortlichen, die erweiterte Zugriffsrechte im Dashboard erhalten, um Benutzerkonten, Lizenzen, Gruppenzuordnungen oder organisatorische Strukturen zu verwalten. Obwohl diese Personen über erhöhte Berechtigungen verfügen, erfolgt kein Zugriff auf Rohdaten, technische Systemdaten oder andere Informationen, die über die zur Verwaltung notwendigen Angaben hinausgehen. Die Verarbeitung beschränkt sich auf die Nutzung administrativer Funktionen, die im Rahmen des Betriebs der Plattform unerlässlich sind.

5. In begrenztem Umfang kann der Auftragsverarbeiter auch personenbezogene Daten seiner eigenen Mitarbeitenden verarbeiten, sofern dies zur Erbringung der vertraglichen Leistungen zwingend erforderlich ist. Hierzu gehören insbesondere Supportmitarbeitende, die Einsicht in technische Supportanfragen benötigen können, Entwickler:innen, die zur Fehlerdiagnose pseudonymisierte Logdaten einsehen, sowie Backend-Administratoren, die in seltenen Fällen technisch notwendige Maßnahmen zur Systemstabilisierung vornehmen. Alle diese Personen sind auf strenge Vertraulichkeit verpflichtet und unterliegen einem detaillierten Berechtigungskonzept, das Zugriffe auf personenbezogene Daten auf das absolut notwendige Maß beschränkt.

6. Darüber hinaus kann es – abhängig von den organisatorischen Vorgaben des Verantwortlichen – vorkommen, dass besondere, optionale Personengruppen betroffen sind. Hierzu zählen etwa Erziehungsberechtigte, sofern deren Kontaktdaten freiwillig vom Verantwortlichen übermittelt werden, etwa zur Kommunikation im Rahmen von Elterninformationen. Ebenso können

Teilnehmende von Workshops, Schulungsmaßnahmen oder Onboarding-Veranstaltungen betroffen sein, sofern deren Namen oder organisatorische Angaben für die Durchführung dieser Formate erforderlich sind. Auch hier gilt, dass die Verarbeitung ausschließlich zweckgebunden erfolgt und nach Abschluss der jeweiligen Maßnahme gelöscht wird.

7. Insgesamt lassen sich die Betroffenengruppen den folgenden Bereichen zuordnen: Lernende, die die App aktiv nutzen und deren Lernfortschritt verarbeitet wird; pädagogische Rollen wie Lehrkräfte und Ausbilder:innen, die Lernprozesse begleiten; administrative Rollen mit eingeschränkter Systemverwaltung; Teilnehmende an Workshops und Schulungen; sowie die Mitarbeitenden des Auftragsverarbeiters, deren Datenverarbeitung ausschließlich zur Vertragserfüllung erforderlich ist.
   Für alle Gruppen gelten die Grundsätze der Datenminimierung, Zweckbindung und Vertraulichkeit. Insbesondere minderjährige Nutzer:innen unterliegen einem erhöhten Schutzniveau, dem durch technische, organisatorische und didaktische Maßnahmen Rechnung getragen wird.

6. Ort der Datenverarbeitung

1. Die Verarbeitung sämtlicher personenbezogener Daten erfolgt ausschließlich innerhalb der Europäischen Union und unterliegt damit vollständig den Bestimmungen der Datenschutz-Grundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG). Der Auftragsverarbeiter stellt sicher, dass sämtliche Systeme, Speicherorte und Serverkomponenten, die im Rahmen der Datenverarbeitung eingesetzt werden, innerhalb der EU betrieben werden und die hierfür erforderlichen technischen und organisatorischen Sicherheitsanforderungen erfüllen.
   Die technische Infrastruktur der BeAFox-Plattform befindet sich vollständig in Deutschland, Region Frankfurt, wodurch gewährleistet ist, dass personenbezogene Daten weder physisch noch logisch außerhalb des europäischen Rechtsraums verarbeitet oder gespeichert werden. Sämtliche Daten werden während der Übertragung und im Ruhezustand verschlüsselt und in hochsicheren, zertifizierten Rechenzentren betrieben.

2. Für das Hosting und den Betrieb der produktiven Systeme nutzt der Auftragsverarbeiter die Dienste von MongoDB Atlas Europe und Render Europe, die beide Serverstandorte in Frankfurt, Deutschland unterhalten. MongoDB speichert sämtliche produktive Nutzer-, Lern- und Metadaten in einem hochverfügbaren

Cluster, das ausschließlich innerhalb der EU betrieben wird und ISO 27001-zertifizierten Sicherheitsstandards entspricht. Die Kommunikation zwischen Backend und Datenbank ist vollständig transportverschlüsselt.
Render Europe betreibt das Backend der Plattform, einschließlich der API, Authentifizierungsprozesse sowie des Systems zur Verwaltung von Benutzerkonten. Auch hier erfolgt die gesamte Verarbeitung personenbezogener Daten ausschließlich innerhalb Deutschlands, ohne jegliche Übermittlung in Drittländer.
Das App-Build-System der Plattform basiert auf Expo/React Native. Dieses System wird ausschließlich zur Erstellung und Bereitstellung von App-Paketen genutzt und verarbeitet zu keinem Zeitpunkt personenbezogene Daten von Endnutzer:innen. Sämtliche personenbezogenen Daten verbleiben ausschließlich im Backend und der Datenbank, sodass weder Expo noch andere Build-Dienste Zugriff auf diese Daten haben. Ein Drittlandtransfer findet hierbei nicht statt.

3. Soweit zur Bereitstellung statischer Inhalte ein Content Delivery Network eingesetzt wird – etwa zur Verbesserung der Ladezeiten oder zur Absicherung gegen Denial-of-Service-Angriffe – erfolgt die Auslieferung ausschließlich über europäische Knotenpunkte. Cloudflare, sofern eingesetzt, betreibt eine EU-Region mit ausschließlich europäischen Endpunkten, die keinen Zugriff auf personenbezogene Inhalte erhält. Es werden keine personenbezogenen Daten gecacht oder dauerhaft gespeichert. Alle über das CDN übertragenen Inhalte sind vollständig verschlüsselt und technisch so gestaltet, dass ein Zugriff durch nicht berechtigte Dritte ausgeschlossen ist.

4. Der Auftragsverarbeiter versichert, dass kein Export personenbezogener Daten in Staaten außerhalb der Europäischen Union stattfindet. Es erfolgt keine Verarbeitung durch Anbieter mit Sitz in Drittländern und keine Übermittlung an Organisationen, die nicht den Anforderungen der DSGVO unterliegen. Insbesondere gelangen keine personenbezogenen Daten an US-amerikanische Anbieter oder Systeme.
Die App-Stores von Apple und Google werden ausschließlich für den Download und die Bereitstellung der App sowie für etwaige Zahlungsabwicklungen verwendet. Sie erhalten zu keinem Zeitpunkt Zugriff auf Lernfortschrittsdaten, pädagogische Informationen oder andere im Backend gespeicherte personenbezogene Daten.

5. Eine Übermittlung personenbezogener Daten in ein Drittland ist nur zulässig, wenn der Verantwortliche zuvor ausdrücklich und schriftlich zugestimmt hat. Darüber

hinaus müssen sämtliche gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sein. Insbesondere muss der Auftragsverarbeiter geeignete Garantien nach Art. 46 DSGVO bereitstellen, wie etwa EU-Standardvertragsklauseln, und ein vollständiges Transfer Impact Assessment (TIA) durchführen. Der Verantwortliche ist über sämtliche Risiken vollständig zu informieren. Ohne die Erfüllung aller genannten Voraussetzungen ist eine Datenübermittlung unzulässig.

6. Um Transparenz und Nachvollziehbarkeit zu gewährleisten, dokumentiert der Auftragsverarbeiter sämtliche Hosting-Dienste, Systemkomponenten, Subunternehmer und technischen Infrastrukturänderungen. Änderungen, die Auswirkungen auf den Ort, die Art oder die Sicherheit der Verarbeitung personenbezogener Daten haben könnten, werden dem Verantwortlichen mindestens 30 Tage vor ihrer Umsetzung schriftlich mitgeteilt. Dies ermöglicht dem Verantwortlichen, rechtzeitig eine Prüfung vorzunehmen oder gegebenenfalls von seinem Widerspruchsrecht Gebrauch zu machen.

7. Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten ausschließlich im Rahmen der gesetzlichen Vorgaben der DSGVO sowie gemäß den dokumentierten Weisungen des Verantwortlichen zu verarbeiten. Er ist nicht berechtigt, die Daten für eigene Zwecke zu nutzen oder Dritten ohne vorherige Zustimmung des Verantwortlichen offenzulegen. Jede Verarbeitung erfolgt ausschließlich im Rahmen des Auftrags, zweckgebunden, datensparsam und unter Anwendung geeigneter technischer und organisatorischer Maßnahmen.

2. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf Grundlage dokumentierter Weisungen des Verantwortlichen. Dies umfasst Vorgaben zu Art, Umfang und technischen Modalitäten der Datenverarbeitung sowie zu Speicherorten, Lösch- und Aufbewahrungsfristen und zur Weitergabe an genehmigte Subunternehmer. Sollte der Auftragsverarbeiter feststellen, dass eine Weisung gegen geltendes Datenschutzrecht verstößt, hat er den Verantwortlichen unverzüglich zu informieren. Rechtswidrige Weisungen werden nicht umgesetzt, bis eine Klärung erfolgt ist.

3. Alle Personen, die beim Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten betraut sind, werden vor Aufnahme ihrer Tätigkeit schriftlich auf Vertraulichkeit verpflichtet und regelmäßig zu relevanten Datenschutz- und Sicherheitsanforderungen geschult. Der Auftragsverarbeiter

stellt sicher, dass der Zugang zu personenbezogenen Daten ausschließlich jenen Mitarbeitenden gewährt wird, deren Tätigkeit dies zwingend erfordert. Zugriffsrechte werden nach dem „Least-Privilege"-Prinzip vergeben, protokolliert, regelmäßig überprüft und bei Rollenwechseln oder dem Ausscheiden von Mitarbeitenden unverzüglich entzogen.

4. Der Auftragsverarbeiter gewährleistet die Sicherheit der Verarbeitung im Sinne von Art. 32 DSGVO durch umfangreiche technische und organisatorische Maßnahmen. Hierzu zählen unter anderem die Verschlüsselung sämtlicher Datenübertragungen und gespeicherter Daten, differenzierte Zugriffs- und Authentifizierungskonzepte, rollenbasierte Berechtigungssysteme, Maßnahmen zur Absicherung der Netzwerke und API-Schnittstellen, regelmäßige Sicherheitsupdates und Patches, Verfahren zur Angriffserkennung sowie umfassende Backup- und Wiederherstellungsmechanismen. Die Wirksamkeit dieser Maßnahmen wird regelmäßig, mindestens einmal jährlich, überprüft und bei Bedarf angepasst.

5. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 24 Stunden, über jede Verletzung des Schutzes personenbezogener Daten oder über jeden begründeten Verdacht einer solchen Verletzung zu informieren. Die Meldung umfasst alle für die Beurteilung des Vorfalls notwendigen Informationen, insbesondere die Art des Vorfalls, die betroffenen Datenkategorien und Personenzahlen, mögliche oder bekannte Folgen sowie die bereits ergriffenen und geplanten Maßnahmen zur Schadensbegrenzung. Der Auftragsverarbeiter unterstützt den Verantwortlichen umfassend bei der Erfüllung seiner gesetzlichen Meldepflichten gegenüber Aufsichtsbehörden und betroffenen Personen.

6. Zur Gewährleistung der Betroffenenrechte gemäß Art. 12 bis 23 DSGVO leistet der Auftragsverarbeiter dem Verantwortlichen unverzüglich und in angemessenem Umfang Unterstützung. Dies umfasst unter anderem die Bereitstellung relevanter Daten, die Umsetzung von Berichtigungs- oder Löschanforderungen, die Einschränkung der Verarbeitung oder die Bereitstellung von Daten in einem maschinenlesbaren Format für Zwecke der Datenübertragbarkeit. Eine direkte Kommunikation mit betroffenen Personen erfolgt durch den Auftragsverarbeiter nur, wenn der Verantwortliche ihn ausdrücklich dazu ermächtigt hat.

7. Nach Beendigung des Hauptvertrags ist der Auftragsverarbeiter verpflichtet, sämtliche personenbezogenen Daten innerhalb von 30 Tagen vollständig und

datenschutzkonform zu löschen oder – sofern der Verantwortliche dies wünscht – zuvor in einem gängigen, maschinenlesbaren und sicher verschlüsselten Format zurückzugeben. Die Löschung wird dokumentiert, und der Auftragsverarbeiter stellt dem Verantwortlichen ein Löschprotokoll zur Verfügung. Daten, die aufgrund gesetzlicher Vorgaben oder technischer Erfordernisse vorübergehend länger gespeichert werden müssen, werden ausschließlich zu diesen Zwecken aufbewahrt und anschließend gelöscht. Backups werden im Rahmen der regulären Lösch- und Überschreibzyklen vernichtet. Eine weitere Verarbeitung personenbezogener Daten nach Vertragsende findet nicht statt.

8. Pflichten des Verantwortlichen

Der Verantwortliche trägt gemäß Art. 4 Nr. 7 DSGVO die Gesamtverantwortung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Er stellt sicher, dass sämtliche Daten, die im Rahmen der Nutzung der BeAFox-Plattform verarbeitet werden, rechtmäßig erhoben, transparent kommuniziert und ausschließlich im Einklang mit den einschlägigen datenschutzrechtlichen Bestimmungen übermittelt werden. Der Verantwortliche hat insbesondere dafür Sorge zu tragen, dass nur solche personenbezogenen Daten an den Auftragsverarbeiter weitergegeben werden, die für die Nutzung der Lernplattform erforderlich sind und deren Verarbeitung auf einer gültigen Rechtsgrundlage beruht. Er gewährleistet zudem, dass keine Daten übermittelt werden, deren Verarbeitung gegen schulrechtliche, behördliche oder gesetzliche Vorgaben verstößt.

Der Verantwortliche erfüllt sämtliche Informationspflichten gegenüber den betroffenen Personen. Alle Lernenden, Lehrkräfte, Administratoren und sonstigen betroffenen Personen müssen in klarer und verständlicher Weise über Art, Zweck und Umfang der Datenverarbeitung unterrichtet werden. Dies umfasst sämtliche Pflichtangaben nach Art. 13 und 14 DSGVO. Der Verantwortliche stellt sicher, dass diese Informationen in geeigneter Weise bereitgestellt werden, etwa durch Datenschutzhinweise, Elterninformationen oder interne Dokumentationen. Die betroffenen Personen sollen jederzeit nachvollziehen können, welche Daten verarbeitet werden und welche Rechte ihnen zustehen.

Werden minderjährige Lernende in die Nutzung einbezogen, trägt der Verantwortliche die Verantwortung dafür, dass eine rechtliche Grundlage im Sinne der DSGVO und des jeweils einschlägigen Schulrechts vorliegt. Dies kann insbesondere eine schulgesetzliche Befugnis, eine behördliche Vorgabe oder eine erforderliche Einwilligung der Erziehungsberechtigten sein. Der Verantwortliche stellt sicher, dass keine überflüssigen personenbezogenen Daten Minderjähriger erhoben werden. Die

Plattform ermöglicht zudem eine datensparsame Nutzung über Alias- oder Pseudonymkonten; der Verantwortliche entscheidet über deren Einsatz.

Der Verantwortliche benennt mindestens eine Ansprechperson für datenschutzbezogene Anliegen und, sofern gesetzlich vorgeschrieben, einen behördlichen oder betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO. Die Kontaktdaten dieser Personen sind dem Auftragsverarbeiter mitzuteilen und stets aktuell zu halten. Ebenso obliegt dem Verantwortlichen die Prüfung und Genehmigung der vom Auftragsverarbeiter eingesetzten Unterauftragsverarbeiter. Er erhält hierzu rechtzeitig die erforderlichen Informationen und hat die Möglichkeit, innerhalb von 30 Tagen datenschutzrechtliche Bedenken zu äußern oder zu widersprechen. Ein Schweigen gilt ausdrücklich nicht als Zustimmung.

Anfragen betroffener Personen, insbesondere zu Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch oder Datenübertragbarkeit, werden ausschließlich durch den Verantwortlichen entgegengenommen und bearbeitet. Der Auftragsverarbeiter leistet hierbei die erforderliche technische Unterstützung, kommuniziert jedoch nicht selbstständig mit den betroffenen Personen, es sei denn, der Verantwortliche erteilt hierzu eine ausdrückliche Weisung.

Der Verantwortliche stellt sicher, dass die Plattform ausschließlich durch autorisierte Nutzer:innen verwendet wird. Er organisiert die sichere Verwaltung von Zugangsdaten, sorgt für die korrekte Vergabe und Zuordnung von Rollen innerhalb der Plattform und stellt sicher, dass interne Prozesse zur sicheren Nutzung existieren. Er gewährleistet, dass unberechtigte Personen keinen Zugang zur App oder zum Dashboard erhalten. Die Verantwortung für die Sicherheit der eigenen IT-Systeme, Endgeräte, Netzwerke und Schul- oder Unternehmensinfrastrukturen liegt vollständig beim Verantwortlichen. Der Auftragsverarbeiter haftet nicht für Sicherheitsmängel in diesen Systemen.

Im Falle eines Datenschutzvorfalls oder eines sicherheitsrelevanten Ereignisses verpflichtet sich der Verantwortliche, unverzüglich mit dem Auftragsverarbeiter zu kooperieren, notwendige Informationen bereitzustellen und eigene interne Prozesse, etwa die Einbindung von Schulleitung, IT-Abteilung oder Datenschutzbeauftragten, zu aktivieren. Er trifft die Entscheidung darüber, ob und in welcher Form eine Meldung an die Aufsichtsbehörde oder an betroffene Personen erforderlich ist.

Schließlich verpflichtet sich der Verantwortliche zur aktiven Zusammenarbeit mit dem Auftragsverarbeiter. Dies umfasst die Bereitstellung aller notwendigen Informationen, die Mitwirkung bei technischen Analysen, die zeitnahe Kommunikation bei

auftretenden Fehlern, Problemen oder Sicherheitsvorfällen sowie die Einhaltung sämtlicher gemeinsam definierter Abläufe und Prozesse, um einen sicheren, rechtskonformen und störungsfreien Betrieb der Plattform zu gewährleisten.

9. Unterauftragsverarbeiter

Der Auftragsverarbeiter ist berechtigt, zur Erfüllung seiner vertraglichen Leistungen Unterauftragsverarbeiter gemäß Art. 28 Abs. 2 und 4 DSGVO einzusetzen. Der Verantwortliche wird über sämtlichen eingesetzten Subunternehmer informiert und hat das Recht, diesen zuzustimmen oder aus wichtigem datenschutzrechtlichem Grund zu widersprechen. Der Auftragsverarbeiter stellt sicher, dass sämtliche Unterauftragsverarbeiter sorgfältig ausgewählt, vertraglich datenschutzkonform verpflichtet und ausschließlich innerhalb der Europäischen Union tätig sind, sodass eine Verarbeitung personenbezogener Daten außerhalb des Geltungsbereichs der DSGVO ausgeschlossen bleibt.

Zum Zeitpunkt des Vertragsabschlusses setzt der Auftragsverarbeiter die folgenden Unterauftragsverarbeiter ein: MongoDB Atlas Europe und Render Europe, jeweils mit Serverstandorten in Frankfurt (Deutschland). MongoDB übernimmt das Hosting und die Speicherung sämtlicher produktiver Daten, darunter Stammdaten, Lern- und Nutzungsdaten sowie technische Metadaten. Die Daten werden ausschließlich in hochverfügbaren Clustern innerhalb der EU gespeichert, die den Anforderungen der ISO 27001 entsprechen und sowohl bei der Übertragung als auch im Ruhezustand verschlüsselt sind. Render Europe betreibt das Backend der Plattform, einschließlich der API-Logik, Authentifizierungsprozesse und der systemrelevanten Funktionen. Auch hier erfolgt die gesamte Verarbeitung innerhalb Deutschlands und ausschließlich zu den vertraglich festgelegten Zwecken.

Das Expo/React-Native-Build-System wird lediglich zur Bereitstellung von App-Paketen verwendet und verarbeitet zu keinem Zeitpunkt personenbezogene Daten der Nutzer:innen. Es handelt sich daher nicht um einen Unterauftragsverarbeiter im Sinne der DSGVO. Sofern zur Verbesserung der Performance ein Content Delivery Network wie Cloudflare eingesetzt wird, erfolgt die Verarbeitung ausschließlich über europäische Endpunkte, ohne dass personenbezogene Daten im Rahmen des Caching oder der Auslieferung gespeichert oder in Drittstaaten übertragen werden. Eine Übermittlung personenbezogener Daten an Cloudflare oder andere externe Netzwerkanbieter findet nicht statt, sofern durch den Verantwortlichen keine abweichenden technischen Anforderungen vorgegeben werden.

Der Auftragsverarbeiter gewährleistet, dass alle Unterauftragsverarbeiter vertraglich verpflichtet werden, angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO umzusetzen, Daten ausschließlich im Rahmen des ihnen übertragenen Auftrags und nach dokumentierten Weisungen zu verarbeiten und keine Verarbeitung in Drittländern vorzunehmen. Ferner stellt der Auftragsverarbeiter sicher, dass Unterauftragsverarbeiter keine weiteren Subdienstleister („Kaskadierung“) ohne ausdrückliche Zustimmung des Auftragsverarbeiters und des Verantwortlichen einsetzen. Sämtliche Subunternehmer müssen regelmäßig Sicherheits-, Compliance- oder Auditberichte vorlegen und ihre Zertifizierungen aktualisieren, damit der Auftragsverarbeiter die fortlaufende DSGVO-Konformität gewährleisten kann. Änderungen in der Subunternehmerstruktur, insbesondere die geplante Hinzunahme eines neuen Unterauftragsverarbeiters, der Austausch eines bestehenden Subunternehmers oder wesentliche Änderungen in Sitz, Struktur oder Verarbeitungsumfang eines Subunternehmers, werden dem Verantwortlichen mindestens 30 Tage im Voraus schriftlich mitgeteilt. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Sollte ein Widerspruch die weitere Erfüllung der vertraglichen Leistung beeinträchtigen, sind beide Parteien verpflichtet, gemeinsam eine Lösung zu erarbeiten. Ist eine Einigung nicht möglich, kann der Verantwortliche den Vertrag aus wichtigem Grund kündigen. Zur Gewährleistung maximaler Transparenz führt der Auftragsverarbeiter ein stets aktuelles Verzeichnis sämtlicher Unterauftragsverarbeiter einschließlich der relevanten Sicherheits- und Compliance-Nachweise, der eingesetzten technischen Systeme und der datenschutzrelevanten Zertifizierungen. Auf Anfrage erhält der Verantwortliche Einsicht in diese Dokumentationen, um seine Kontroll- und Prüfpflichten gemäß Art. 28 DSGVO wahrnehmen zu können.

10. Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter verpflichtet sich, angemessene technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO sicherzustellen. Die Maßnahmen werden regelmäßig überprüft, aktualisiert und dokumentiert. Nachstehend werden alle relevanten TOMs detailliert beschrieben.

10.1 Organisatorische Sicherheitsmaßnahmen

Der Auftragsverarbeiter betreibt ein umfassendes Datenschutz- und Informationssicherheitsmanagement, das sich an den Vorgaben der DSGVO sowie

bewährten Standards wie ISO 27001 und dem BSI-Grundschutz orientiert. Sämtliche Prozesse zur Verarbeitung personenbezogener Daten erfolgen innerhalb einer klar strukturierten organisatorischen Sicherheitsarchitektur, deren Zweck es ist, Transparenz, Verantwortlichkeit und ein dauerhaft hohes Schutzniveau zu gewährleisten.

Zentrale Grundlage hierfür ist eine eindeutige Definition der internen Verantwortlichkeiten. Rollen wie Entwicklung, Support, Administration und Management sind klar voneinander abgegrenzt und werden in einer dokumentierten Rollenmatrix festgehalten. Diese Matrix legt fest, welche Mitarbeitenden welche Aufgaben durchführen dürfen und welche Zugriffsbefugnisse hierfür erforderlich sind. Jede Rolle ist so gestaltet, dass sie nur den minimal notwendigen Zugang zu Daten erhält.

Alle Mitarbeitenden, die im Rahmen ihrer Tätigkeit mit personenbezogenen Daten in Berührung kommen, werden vor Aufnahme ihrer Tätigkeit und regelmäßig im Verlauf ihrer Beschäftigung auf Vertraulichkeit verpflichtet. Diese Verpflichtung umfasst insbesondere die Pflicht zur Beachtung aller Datenschutz- und Sicherheitsvorgaben sowie den sorgfältigen Umgang mit sensiblen Informationen.

Der Auftragsverarbeiter verfügt über ein internes Datenschutz- und Sicherheitskonzept, das den organisatorischen und technischen Rahmen der Datenverarbeitung beschreibt. Es beinhaltet unter anderem Richtlinien zur Datenminimierung, Löschung, Zugriffskontrolle, Incident Response, Backup sowie Entwicklungsprozesse. Dieses Konzept wird laufend angepasst und mindestens einmal jährlich überprüft.

Regelmäßige interne Audits stellen sicher, dass alle Prozesse den rechtlichen Vorgaben und den eigenen Standards entsprechen. Abweichungen werden dokumentiert und zeitnah behoben. Ergänzend werden kontinuierlich Risikobewertungen durchgeführt, die die Sicherheit der Systeme sowie die möglichen Auswirkungen auf die Betroffenen berücksichtigen. Neue Risiken werden durch entsprechende Maßnahmen reduziert, bevor sie operative Relevanz erlangen können.

10.2 Technische Maßnahmen zur Zugriffskontrolle

Der Auftragsverarbeiter stellt durch umfassende technische Mechanismen sicher, dass der Zugriff auf Systeme und personenbezogene Daten ausschließlich autorisierten Personen vorbehalten ist. Die Zugriffskontrolle folgt einem strengen

Sicherheitsmodell, das sowohl technische als auch organisatorische Maßnahmen kombiniert.

Der Zugang zu sämtlichen Systemen erfolgt ausschließlich über gesicherte Authentifizierungsmechanismen. Passwörter werden niemals im Klartext gespeichert, sondern ausschließlich in gehashter Form unter Verwendung moderner, kryptografisch sicherer Hashverfahren. Administrative Zugänge, Backend-Systeme sowie kritische Managementbereiche sind zusätzlich durch eine Mehr-Faktor-Authentifizierung geschützt, um unbefugte Zugriffe auch im Fall von Passwortkompromittierungen auszuschließen.

Zudem existieren strenge Beschränkungen des Systemzugangs. Administrative Oberflächen, Datenbankzugänge und technische Konfigurationsschnittstellen sind nicht öffentlich zugänglich und befinden sich in isolierten Netzwerken. Der Zugang zu diesen Bereichen erfolgt ausschließlich über VPN oder dedizierte Netzwerkzugänge mit IP-Whitelist-Regelungen. Entwicklerinnen und Entwickler haben keinen direkten Zugriff auf produktive Nutzerdaten und arbeiten ausschließlich mit Test- oder Dummy-Daten.

Sämtliche Zugriffe, die sicherheitsrelevant sein könnten, werden umfassend protokolliert. Dies betrifft insbesondere Anmeldevorgänge, Rollenänderungen, administrative Aktionen und ungewöhnliche API-Aktivitäten. Die Protokolle werden manipulationsgeschützt gespeichert und regelmäßig ausgewertet. Auf Grundlage dieser Auswertungen werden Auffälligkeiten identifiziert und gegebenenfalls Sicherheitsmaßnahmen eingeleitet.

Die Zugriffskontrolle wird durch ein fein abgestuftes Berechtigungskonzept ergänzt, das sicherstellt, dass jede Person nur diejenigen Daten einsehen kann, die für ihre Tätigkeit erforderlich sind. Die Rechteverwaltung basiert auf einem rollenbasierten Modell, das Zugriffe klar voneinander trennt und verhindert, dass Personen Einblick in Daten anderer Nutzergruppen oder Mandanten erhalten. Rechte werden regelmäßig überprüft und bei Rollenwechseln oder Austritten unverzüglich entzogen.

10.3 Netzwerksicherheit & API-Sicherheit

Der physische Zutritt zu den Systemen, in denen personenbezogene Daten verarbeitet oder gespeichert werden, ist durch strenge technische und organisatorische Maßnahmen geschützt. Die gesamte Serverinfrastruktur von BeAFox wird ausschließlich in professionellen, ISO-27001-zertifizierten Rechenzentren innerhalb

Deutschlands (Region Frankfurt) betrieben, die modernste Sicherheitsstandards erfüllen.

Der Zutritt zu diesen Rechenzentren ist auf einen eng begrenzten Personenkreis beschränkt und erfolgt ausschließlich über mehrstufige Sicherheitsmechanismen. Dazu gehören insbesondere persönliche Zugangsausweise, biometrische Merkmale und Sicherheitsschleusen, die sicherstellen, dass nur autorisierte Personen die Serverräume betreten können. Jede Zutrittsbewegung wird protokolliert und zentral überwacht.

Die Rechenzentren verfügen über umfangreiche physische Sicherheitsvorkehrungen zum Schutz vor Diebstahl, Vandalismus, Sabotage, Feuer und Naturkatastrophen. Dazu zählen unter anderem Brandfrüherkennungssysteme, Gaslöschanlagen, doppelte Energieversorgung, Notstromaggregate sowie redundante Netzwerkverbindungen.

Der Auftragsverarbeiter selbst hat keinen physischen Zugang zu den Servern. Der Zugriff erfolgt ausschließlich über abgesicherte digitale Schnittstellen. Dadurch wird sichergestellt, dass personenbezogene Daten nicht durch unbefugte physische Manipulation gefährdet werden.

Darüber hinaus wird die Infrastruktur rund um die Uhr überwacht, sodass sicherheitsrelevante Vorfälle oder ungewöhnliche Aktivitäten sofort erkannt und behoben werden können. Durch diese Maßnahmen wird ein Höchstmaß an physischer Sicherheit gewährleistet, das den gesetzlichen Anforderungen sowie den Erwartungen öffentlicher Einrichtungen entspricht.

10.4 Maßnahmen zur Datentrennung

Der Auftragsverarbeiter stellt durch eine Vielzahl technischer Maßnahmen sicher, dass sämtliche Netzwerkverbindungen und API-Schnittstellen gegen unbefugte Zugriffe und Manipulationen geschützt sind. Sämtliche Kommunikationswege zwischen App, Dashboard, Backend und Datenbank werden ausschließlich über verschlüsselte Verbindungen mittels TLS 1.2 oder höher übertragen. Unsichere Verbindungen werden serverseitig strikt abgewiesen. Durch Aktivierung von HSTS wird sichergestellt, dass Endgeräte ausschließlich HTTPS-Verbindungen zulassen, wodurch die Gefahr von Downgrade- und Man-in-the-Middle-Angriffen wirksam ausgeschlossen wird.

Die APIs der Plattform unterliegen einer kontinuierlichen Sicherheitsüberwachung. Um Angriffe wie Brute-Force, Credential Stuffing oder missbräuchliche Massenanfragen

zu verhindern, setzt der Auftragsverarbeiter dynamisches Rate-Limiting sowie Throttling-Mechanismen ein. Darüber hinaus werden API-Zugriffe ausschließlich von autorisierten Ursprungsdomänen akzeptiert. Eine restriktiv konfigurierte CORS-Policy verhindert, dass nicht autorisierte Webseiten oder Dienste Anfragen an das Backend stellen können.

Zum Schutz der Systeme vor Angriffen auf Anwendungsebene setzt der Auftragsverarbeiter zusätzlich eine Web Application Firewall ein, sofern der Einsatz im jeweiligen Mandantenumfeld vorgesehen ist. Diese analysiert und filtert schädliche oder ungewöhnliche Anfragen, blockiert verdächtige Zugriffsmuster und schützt insbesondere vor Angriffen wie Cross-Site-Scripting, SQL- bzw. NoSQL-Injection, Command Injection und DDoS-Angriffen.
Darüber hinaus werden sämtliche Netzwerkverbindungen durch Firewalls abgesichert, welche ausschließlich zwingend erforderliche Ports freigeben. Interne Dienste und Verwaltungsoberflächen sind nicht öffentlich erreichbar und sind in private Netzwerksegmente isoliert.

Die Nutzung der API wird in Echtzeit überwacht. Dabei werden auffällige Muster wie erhöhte Frequenzen, ungewöhnliche Zugriffszeiten, geographisch untypische Anfragen oder Zugriffe auf sensible Endpunkte automatisiert erkannt. Bei Auffälligkeiten können Tokens automatisiert gesperrt und Angriffe sofort unterbunden werden.

10.5 Maßnahmen zur Sicherung der Integrität

Der Auftragsverarbeiter gewährleistet, dass sämtliche Daten strikt getrennt verarbeitet werden und kein unbefugter Datenfluss zwischen verschiedenen Verantwortlichen oder Systemen stattfindet. Hierzu betreibt der Auftragsverarbeiter vollständig voneinander isolierte Entwicklungs-, Test- und Produktionsumgebungen. Produktivdaten werden ausschließlich in der Produktionsumgebung verarbeitet; ein Transfer produktiver personenbezogener Daten in Test- oder Entwicklungsumgebungen ist untersagt und technisch unterbunden. Testumgebungen verwenden ausschließlich künstliche oder anonymisierte Daten.

Die Daten verschiedener Mandanten wie Schulen oder Unternehmen werden logisch voneinander getrennt, etwa durch separate Datenbankstrukturen oder Mandantenkennungen. Dadurch wird sichergestellt, dass Personen aus einem Mandantenkreis keinerlei Einsicht in Daten eines anderen Mandanten erhalten können.

Auch innerhalb der Benutzeroberflächen wie dem Dashboard erfolgt eine strikte Rollen- und Berechtigungslogik. Lehrkräfte oder Ausbilder haben ausschließlich Zugriff auf die ihnen zugewiesenen Lernenden bzw. Gruppen. Administrierende Rollen können nur jene Daten einsehen, die für ihre Funktion zwingend erforderlich sind. Damit wird die Trennung der Daten auf technischen, organisatorischen und funktionalen Ebenen gewährleistet.

10.6 Maßnahmen zur Sicherung der Verfügbarkeit

Zur Sicherstellung der Datenintegrität setzt der Auftragsverarbeiter umfangreiche Maßnahmen ein, die gewährleisten, dass Daten weder unbeabsichtigt noch unbefugt verändert werden können. Sämtliche Eingaben, die durch Nutzer oder Systeme erfolgen, werden serverseitig auf Gültigkeit, Struktur, Datentyp und erwartetes Verhalten geprüft. Dadurch werden sowohl technische Fehler als auch Sicherheitsrisiken minimiert.

Die Integrität aller übertragenen Daten wird durch moderne kryptografische Verfahren geschützt. Daten werden ausschließlich verschlüsselt übertragen und unterliegen Prüfsummen oder Signaturverfahren, die Manipulationen erkennen.

Um Angriffe auf Anwendungsebene zu verhindern, verwendet der Auftragsverarbeiter Schutzmechanismen gegen Cross-Site-Scripting, Cross-Site-Request-Forgery, SQL-/NoSQL-Injection, Deserialisierungsangriffe und andere gängige Angriffsmethoden. Eine strikte serverseitige Validierung stellt sicher, dass nur eindeutig zulässige Befehle oder Eingaben akzeptiert werden.

Änderungen am Quellcode durchlaufen standardisierte Peer-Review-Verfahren. Jede Änderung muss von qualifizierten Teammitgliedern geprüft, freigegeben und dokumentiert werden. Der gesamte Entwicklungsprozess ist versioniert und ermöglicht Nachvollziehbarkeit sämtlicher Änderungen. Dadurch können Fehlerquellen identifiziert und frühzeitig korrigiert werden.

10.7 Backup- und Wiederherstellungsverfahren

Der Auftragsverarbeiter betreibt seine Infrastruktur so, dass eine hohe Verfügbarkeit der Systeme gewährleistet ist. Die produktive Datenbank wird als mehrknotiges Replikationscluster betrieben, das bei Ausfall eines Knotens automatisch auf einen anderen Knoten übergeht (Failover). Zusätzlich werden redundante Serverstrukturen innerhalb der Europäischen Union betrieben, die eine Fortführung des Betriebs selbst unter schwierigen Bedingungen möglich machen.

Zur Sicherung gegen Angriffe auf die Verfügbarkeit werden DDoS-Schutzmechanismen eingesetzt, die automatisiert ungewöhnlichen Traffic erkennen und blockieren. Sämtliche Systeme werden kontinuierlich hinsichtlich Auslastung, Netzwerkverbindungen, Speicherverbrauch, Latenz und API-Gesundheit überwacht. Bei Überschreiten definierter Schwellenwerte werden interne Alarmierungen ausgelöst, sodass technische Teams reagieren können.

Die Infrastruktur ist skalierbar und passt sich automatisiert an veränderte Lastsituationen an. Damit können auch hohe Zugriffszahlen oder Belastungsspitzen ohne Funktionsverlust verarbeitet werden. Geplante Wartungsarbeiten erfolgen nur nach vorheriger Ankündigung und werden nach Möglichkeit außerhalb kritischer Nutzungszeiten durchgeführt.

Zielwerte:

RPO: ≤ 24 Stunden

RTO: ≤ 48 Stunden

10.8 Maßnahmen bei Sicherheitsvorfällen (Incident Response)

Der Auftragsverarbeiter verfügt über einen dokumentierten Incident-Response-Plan, der festlegt, wie Sicherheitsvorfälle erkannt, analysiert, eingedämmt und behoben werden. Sobald ein Vorfall entdeckt wird oder ein begründeter Verdacht besteht, werden unverzüglich interne Maßnahmen zur Schadensbegrenzung eingeleitet. Dazu gehört die Isolierung betroffener Systeme, die Unterbindung unerlaubter Zugriffe sowie die Sicherung relevanter Log- und Systemdaten für die spätere Analyse.

Eine forensische Auswertung wird durchgeführt, um den Ursprung, den Ablauf und die Auswirkungen des Vorfalls festzustellen. Das Ergebnis wird vollständig dokumentiert und dient nicht nur der Aufklärung, sondern auch der Verbesserung zukünftiger Sicherheitsmaßnahmen („Lessons Learned“).

Der Verantwortliche wird spätestens innerhalb von 24 Stunden informiert, sobald ein Vorfall Auswirkungen auf personenbezogene Daten haben könnte oder eine Verletzung des Schutzes personenbezogener Daten nicht ausgeschlossen werden kann. Der Auftragsverarbeiter unterstützt den Verantwortlichen aktiv bei der Erfüllung etwaiger Meldepflichten gegenüber Aufsichtsbehörden und Betroffenen gemäß Art. 33 und 34 DSGVO.

10.9 Maßnahmen zur Löschung und Datenminimierung

Der Auftragsverarbeiter setzt technische und organisatorische Verfahren ein, die die Einhaltung des Grundsatzes der Datenminimierung gewährleisten. Personenbezogene Daten werden nur so lange gespeichert, wie sie zur Erfüllung des Vertragszwecks erforderlich sind. Konten inaktiver Nutzerinnen und Nutzer können automatisch nach den Vorgaben des Verantwortlichen gelöscht oder anonymisiert werden.

Nach Beendigung des Vertragsverhältnisses werden sämtliche personenbezogenen Daten innerhalb von 30 Tagen vollständig gelöscht. Der Verantwortliche kann zuvor die Herausgabe aller Daten in maschinenlesbarer Form verlangen, etwa als CSV- oder JSON-Datei.

Backups, die personenbezogene Daten enthalten könnten, werden im Rahmen des regulären Backup-Zyklus automatisch überschrieben und so nachträglich gelöscht. Neue Funktionen werden nach dem Prinzip der datenschutzfreundlichen Voreinstellung (Privacy by Default) und datenschutzfreundlichen Technikgestaltung (Privacy by Design) entwickelt, sodass nur die minimal erforderlichen Daten verarbeitet werden.

10.10 Besondere Maßnahmen zum Schutz Minderjähriger (falls zutreffend)

Da die Plattform BeAFox häufig von minderjährigen Nutzern verwendet wird, gelten besonders strenge Schutzmaßnahmen. Nutzerkonten können vollständig pseudonym betrieben werden; die Verarbeitung von Klarnamen ist nur dann erforderlich, wenn der Verantwortliche diese übermittelt.

Die Plattform erhebt keine Standortdaten, Gesundheitsdaten, biometrischen Daten oder andere besonders schutzwürdige Informationen Minderjähriger. Ebenso verzichtet der Auftragsverarbeiter vollständig auf Werbung, Trackingmechanismen, Profilbildung oder jede Form der kommerziellen Weitergabe von Nutzungsdaten.

Das Dashboard zeigt Lehrkräften ausschließlich die für pädagogische Zwecke erforderlichen Daten an, etwa Lernfortschritte oder Bearbeitungsstände. Private Nutzungsdaten oder Verhaltensanalysen werden nicht dargestellt.

Für minderjährige Nutzer bestehen besonders restriktive Voreinstellungen. Die App ist so gestaltet, dass Datenschutzrisiken minimiert und Sicherheitsfunktionen standardmäßig aktiviert sind.

§11 Zusammenarbeit mit Aufsichtsbehörden

Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen bei sämtlichen Anfragen, Prüfungen, Untersuchungen oder sonstigen Maßnahmen durch Datenschutzaufsichtsbehörden gemäß Art. 31 DSGVO umfassend zu unterstützen. Diese Unterstützung erstreckt sich auf alle Situationen, in denen die Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung der BeAFox-Plattform Gegenstand aufsichtsbehördlicher Maßnahmen ist.

Die Unterstützungspflichten des Auftragsverarbeiters umfassen insbesondere:

Bereitstellung technischer und organisatorischer Dokumentationen
Der Auftragsverarbeiter stellt dem Verantwortlichen alle Unterlagen, Nachweise und technischen Beschreibungen zur Verfügung, die für die Bewertung oder Prüfung der Datenverarbeitung durch die Aufsichtsbehörde erforderlich sind.

Dazu gehören unter anderem:

- Dokumentationen zu den eingesetzten Sicherheitsmaßnahmen,
- Prozessbeschreibungen,
- Protokolle relevanter Ereignisse,
- Informationen zu Subunternehmern,
- Architekturübersichten der Plattform.

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit fachlichen, technischen und organisatorischen Informationen, damit Anfragen der Aufsichtsbehörde vollständig, korrekt und fristgerecht beantwortet werden können.
Dies umfasst auch die Erstellung technischer Stellungnahmen und die Durchführung notwendiger Analysen.

Mitwirkung bei der Aufklärung von Vorfällen oder Beschwerden
Im Falle datenschutzbezogener Beschwerden betroffener Personen, sicherheitsrelevanter Vorfälle oder behördlich angeordneter Prüfungen unterstützt der

Der Auftragsverarbeiter führt keine direkte Kommunikation mit Aufsichtsbehörden, sofern der Verantwortliche nicht ausdrücklich eine entsprechende Weisung erteilt hat oder eine gesetzliche Verpflichtung zur direkten Auskunft besteht (z. B. im Rahmen einer unmittelbaren Anfrage nach Art. 31 DSGVO).
In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich über Inhalt und Umfang der behördlichen Anfrage.

Der Auftragsverarbeiter sorgt dafür, dass alle erforderlichen Informationen und Unterlagen rechtzeitig bereitgestellt werden, damit der Verantwortliche gesetzliche

Fristen gegenüber der Aufsichtsbehörde einhalten kann.
Der Auftragsverarbeiter verpflichtet sich, interne Prozesse so zu gestalten, dass eine zeitnahe und sachgerechte Zusammenarbeit gewährleistet ist.

Durch diese Maßnahmen wird sichergestellt, dass der Verantwortliche seinen gesetzlichen Verpflichtungen gegenüber Datenschutzaufsichtsbehörden ordnungsgemäß nachkommen kann und eine transparente, sichere und rechtskonforme Verarbeitung gewährleistet bleibt.

§12. Kontrollrechte des Verantwortlichen

1. Der Verantwortliche ist gemäß Art. 28 DSGVO berechtigt, die Einhaltung der gesetzlichen Anforderungen sowie der in diesem Vertrag vereinbarten technischen und organisatorischen Maßnahmen jederzeit zu überprüfen oder durch geeignete Dritte überprüfen zu lassen. Diese Kontrollen dienen der Sicherstellung, dass der Auftragsverarbeiter alle Verpflichtungen aus der DSGVO und diesem Vertrag ordnungsgemäß erfüllt.

2. Der Auftragsverarbeiter unterstützt den Verantwortlichen aktiv bei der Wahrnehmung dieser Kontrollrechte. Er stellt die erforderlichen Informationen, Nachweise und Dokumentationen zur Verfügung, die es dem Verantwortlichen ermöglichen, die datenschutzkonforme Verarbeitung nachzuvollziehen. Dazu gehören insbesondere technische Beschreibungen, Prozessdokumentationen, Sicherheitskonzepte, Berechtigungsübersichten, Auditberichte und Protokolle wesentlicher Sicherheitsereignisse.

3. Kontrollen können grundsätzlich in den Räumlichkeiten des Verantwortlichen oder – sofern erforderlich – in den Räumlichkeiten des Auftragsverarbeiters oder seiner Unterauftragsverarbeiter stattfinden. Der Auftragsverarbeiter verpflichtet sich, solche Kontrollen in angemessenem Umfang zu ermöglichen und dafür Sorge zu tragen, dass die Teilnahme keine Gefährdung der Sicherheit oder Verfügbarkeit der Systeme zur Folge hat. Der Verantwortliche trägt dafür Sorge, dass Kontrollen rechtzeitig angekündigt werden, sofern keine Gefahr im Verzug besteht.

4. Soweit möglich, stellt der Auftragsverarbeiter dem Verantwortlichen statt eines physischen Audits geeignete Nachweise wie Zertifizierungen, externe Prüfberichte (z. B. ISO 27001, SOC2) oder standardisierte Audit-Fragebögen zur Verfügung. Der Verantwortliche ist verpflichtet, solche standardisierten Nachweise anzuerkennen,

sofern sie den Anforderungen des Art. 28 DSGVO und den vertraglichen Bestimmungen genügen.

5. Der Verantwortliche hat das Recht, sich vor Ort oder durch elektronische Einsichtnahme von der Wirksamkeit der technischen und organisatorischen Maßnahmen zu überzeugen. Dabei verpflichtet sich der Verantwortliche, die berechtigten Interessen des Auftragsverarbeiters, insbesondere Betriebs- und Geschäftsgeheimnisse sowie Schutzrechte hinsichtlich der Sicherheitssysteme, zu berücksichtigen. Kontrollen dürfen die Betriebsabläufe des Auftragsverarbeiters nicht unangemessen beeinträchtigen.

6. Stellt der Verantwortliche im Rahmen einer Kontrolle Mängel fest, wird der Auftragsverarbeiter unverzüglich geeignete Maßnahmen zur Behebung ergreifen. Der Auftragsverarbeiter dokumentiert die umgesetzten Maßnahmen und teilt sie dem Verantwortlichen mit. Sicherheitskritische Vorfälle, relevante Systemänderungen, die Einführung neuer Unterauftragsverarbeiter oder wesentliche Anpassungen der TOMs werden dem Verantwortlichen rechtzeitig mitgeteilt, sodass dieser sein Kontrollrecht wirksam ausüben kann.

§ 13. Weisungen

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisungen des Verantwortlichen. Dies entspricht den Vorgaben des Art. 28 Abs. 3 lit. a DSGVO. Weisungen können sich sowohl auf Art, Umfang und Zwecke der Datenverarbeitung als auch auf besondere technische oder organisatorische Maßnahmen beziehen, sofern diese mit dem Vertragszweck vereinbar sind.

2. Alle Weisungen müssen in Textform erfolgen, es sei denn, eine mündliche oder telefonische Weisung ist aufgrund besonderer Umstände kurzfristig erforderlich. In solchen Ausnahmefällen ist der Verantwortliche verpflichtet, die mündliche Weisung unverzüglich nachträglich in Textform zu bestätigen. Der Auftragsverarbeiter führt Weisungen erst dann aus, wenn sie eindeutig und dokumentiert vorliegen. Der Auftragsverarbeiter ist verpflichtet, jede Weisung zu prüfen und den Verantwortlichen unverzüglich zu informieren, wenn nach Auffassung des Auftragsverarbeiters eine Weisung datenschutzrechtlich unzulässig ist oder zu einer rechtswidrigen Verarbeitung führen würde. In solchen Fällen wird die Ausführung der Weisung bis zur Klärung ausgesetzt. Eine Haftung für die Ausführung rechtswidriger Weisungen besteht für den Auftragsverarbeiter

nicht. Der Verantwortliche ist berechtigt, jederzeit neue Weisungen zu erteilen oder bestehende Weisungen zu ändern, sofern diese den vertraglich vereinbarten Leistungsumfang nicht verändern. Änderungen, die den Umfang, die Art oder die technischen Grundvoraussetzungen der Verarbeitung wesentlich berühren, bedürfen einer ergänzenden vertraglichen Vereinbarung.

3. Der Auftragsverarbeiter dokumentiert sämtliche Weisungen und deren Umsetzung. Auf Wunsch stellt er dem Verantwortlichen eine Übersicht der erteilten Weisungen zur Verfügung. Sämtliche Personen, die beim Auftragsverarbeiter mit der Datenverarbeitung betraut sind, werden intern angewiesen, ausschließlich dokumentierte Weisungen auszuführen. Sofern eine Weisung technisch nicht umsetzbar, unverhältnismäßig oder für den Auftragsverarbeiter unzumutbar ist, wird dies dem Verantwortlichen unverzüglich mitgeteilt. Beide Parteien verpflichten sich, in solchen Fällen gemeinsam eine Lösung zu erarbeiten, die den Anforderungen der DSGVO entspricht und gleichzeitig den operativen Betrieb der Plattform nicht beeinträchtigt.

§ 14. Verschwiegenheit

1. Der Auftragsverarbeiter verpflichtet sich, sämtliche ihm im Rahmen der Auftragsverarbeitung bekannt werdenden personenbezogenen Daten sowie alle sonstigen Informationen, die ihm vom Verantwortlichen zugänglich gemacht werden oder im Rahmen der Durchführung dieses Vertrages entstehen, streng vertraulich zu behandeln. Eine Weitergabe an Dritte ist nur zulässig, sofern sie durch diesen Vertrag ausdrücklich gestattet ist oder eine gesetzliche Verpflichtung hierzu besteht.

2. Alle Mitarbeitenden des Auftragsverarbeiters, die Zugang zu personenbezogenen Daten erhalten, sind vor Aufnahme ihrer Tätigkeit schriftlich auf Vertraulichkeit verpflichtet worden. Diese Verpflichtung umfasst insbesondere die Einhaltung der datenschutzrechtlichen Vorschriften, die Geheimhaltung personenbezogener Daten sowie das Verbot der unbefugten Nutzung, Weitergabe oder Offenlegung solcher Daten. Der Auftragsverarbeiter verpflichtet sich, diese Verpflichtung regelmäßig zu überprüfen und bei Bedarf zu aktualisieren.

3. Die Pflicht zur Verschwiegenheit erstreckt sich auf alle Informationen, die dem Auftragsverarbeiter im Rahmen der Zusammenarbeit bekannt werden, einschließlich technischer Dokumentationen, pädagogischer oder organisatorischer Informationen des Verantwortlichen, Unterrichts- und

Ausbildungsstrukturen sowie sämtlicher personenbezogener Daten von Lernenden, Beschäftigten und sonstigen Betroffenen.

4. Die Verschwiegenheitspflicht gilt zeitlich unbegrenzt und bleibt auch nach Beendigung des Vertragsverhältnisses bestehen. Der Auftragsverarbeiter stellt sicher, dass vertrauliche Informationen zu keinem Zeitpunkt für eigene Zwecke genutzt oder Dritten zugänglich gemacht werden, sofern keine ausdrückliche Einwilligung oder gesetzliche Verpflichtung vorliegt. Soweit der Auftragsverarbeiter zur Erfüllung seiner vertraglichen Pflichten externe Dienstleister (Unterauftragsverarbeiter) einsetzt, stellt er sicher, dass diese denselben hohen Vertraulichkeitsanforderungen unterliegen. Dies umfasst insbesondere die Verpflichtung, vertrauliche Informationen ausschließlich auf dokumentierte Weisung des Auftragsverarbeiters zu verarbeiten und die Daten nicht für eigene Zwecke zu nutzen.

5. Verstöße gegen diese Verschwiegenheitspflicht sind dem Verantwortlichen unverzüglich mitzuteilen. Der Auftragsverarbeiter ist verpflichtet, geeignete Maßnahmen zu ergreifen, um die Auswirkungen eines solchen Verstoßes zu begrenzen und zukünftige Verstöße zu verhindern.

§ 14. Vertragsdauer

1. Dieser Auftragsverarbeitungsvertrag tritt mit Unterzeichnung durch beide Parteien in Kraft und gilt für die gesamte Dauer des zwischen den Parteien bestehenden Lizenz- bzw. Nutzungsvertrags über die Lernplattform BeAFox. Er endet automatisch mit dem Ende des Hauptvertrags, ohne dass es einer gesonderten Kündigung bedarf.

2. Die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ist ausschließlich für die Dauer des Hauptvertrags gestattet. Nach dessen Beendigung ist der Auftragsverarbeiter verpflichtet, sämtliche personenbezogenen Daten gemäß den Regelungen dieses Vertrages zu löschen oder – sofern dies durch den Verantwortlichen gewünscht und beauftragt wurde – in einem maschinenlesbaren Format zurückzugeben.

3. Nach dem Ende des Hauptvertrags beginnt eine Nachlaufphase von 30 Tagen, innerhalb derer der Verantwortliche entscheiden kann, ob Daten zurückgegeben

werden sollen. Während dieser Phase findet keine weitere Verarbeitung von personenbezogenen Daten statt, es sei denn, dies ist zur Erfüllung gesetzlicher Aufbewahrungspflichten oder zur sicheren Durchführung der Löschung erforderlich. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen die ordnungsgemäße Löschung in Form eines Löschprotokolls nachzuweisen. Mit Abschluss dieser Nachlaufphase gelten alle datenschutzrechtlichen Verpflichtungen aus der fortdauernden Verarbeitung als beendet, unbeschadet weiterbestehender Vertraulichkeitspflichten.

4. Sollte der Hauptvertrag aus wichtigem Grund außerordentlich gekündigt werden, endet dieser Auftragsverarbeitungsvertrag gleichzeitig. Die Verpflichtungen zur Löschung, Herausgabe und Verschwiegenheit bleiben hiervon unberührt.

§ 15. Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses selbst. Mündliche Nebenabreden bestehen nicht. Änderungen der vertraglichen Grundlagen oder der technischen und organisatorischen Maßnahmen werden vom Auftragsverarbeiter dokumentiert und dem Verantwortlichen auf Wunsch zur Verfügung gestellt.

2. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch eine solche zu ersetzen, die dem wirtschaftlichen Zweck sowie den datenschutzrechtlichen Anforderungen in rechtlich zulässiger Weise am nächsten kommt. Gleiches gilt für etwaige Regelungslücken.

3. Der Auftragsverarbeiter ist nicht berechtigt, diesen Vertrag oder Teile seiner Verpflichtungen, ohne vorherige schriftliche Zustimmung des Verantwortlichen auf Dritte zu übertragen. Dies gilt nicht für den Einsatz genehmigter Unterauftragsverarbeiter gemäß den in diesem Vertrag enthaltenen Regelungen. Soweit in diesem Vertrag nichts Abweichendes geregelt ist, gelten ergänzend die Bestimmungen des zwischen den Parteien bestehenden Hauptvertrags (Lizenzvertrag). Bei Widersprüchen zwischen dem Hauptvertrag und diesem Auftragsverarbeitungsvertrag gehen die Regelungen dieses Vertrages vor, soweit sie datenschutzrechtliche Aspekte betreffen.

4. Für diesen Vertrag gilt ausschließlich des Rechts der Bundesrepublik Deutschland unter Ausschluss internationaler Kollisionsnormen und des UN-Kaufrechts. Ausschließlicher Gerichtsstand für alle Streitigkeiten im Zusammenhang mit diesem Vertrag ist – soweit gesetzlich zulässig – der Sitz des Verantwortlichen. Sind abweichende internationale Zuständigkeiten gesetzlich ausgeschlossen, gilt der Sitz des Auftragsverarbeiters.

5. Dieser Vertrag ersetzt sämtliche vorherigen Vereinbarungen zum Gegenstand der Auftragsverarbeitung. Er tritt mit seiner Unterzeichnung durch beide Parteien in Kraft und gilt für die gesamte Dauer der Datenverarbeitung im Rahmen des Hauptvertrags.

Unterschriften[1]

---	
Ort, Datum des Lizenznehmers	Alexandru Tapelea, BeAFox