Für Ihre Datenschutz-Unterlagen. Rücksendung ist nicht erforderlich!

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen

Testschule Musterstadt2 Grund- und Gemeinschaftsschule

Testschule Musterstadt

Schulstr. 1

12345 Musterstadt

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

atenis GmbH

Danziger Str. 20

72116 Mössingen

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Musterstadt, den 10. September 2018

Ort, Datum

Mössingen, den 10. September 2018

Ort, Datum

Harri Pallas (Geschäftsführer atenis GmbH)

Anlagen:

- Allgemeine technische und organisatorische Maßnahmen nach Art. 32 EU-DSGVO
- Zertifikat nach ISO/IEC 27001 der Hetzner Online GmbH
- Risikoeinstufung der KI-Funktion

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand: Der Gegenstand des Auftrags ist die Bereitstellung eines Online-Portals zur Erfassung und Erstellung von Lernentwicklungsberichten auf zeufix.de und der aktuell gültigen AGB von zeufix.de auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung). Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(2) Dauer: Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 10 Tagen zum Ende des Abrechnungszeitraumes ordentlich gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in den AGB und der Dokumentation der Verarbeitungstätigkeit.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in Deutschland wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten von Schülern (Name, Geburtsdatum, Geburtsort)
- ☐ Personenstammdaten von Lehrern (Name)
- ☐ Kommunikationsdaten (E-Mail)
- ☐ erfasste Schülerleistungen (Verbalbeurteilungen, Noten, sonst. Beurteilungen, Lernentwicklungsberichte)

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Lehrer
- ☐ Schüler

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Harri Pallas, Tel: 07473/951341 h.pallas@atenis.de benannt.
b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen

Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
(2) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt.
(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gem. Art. 28 DS-GVO und nur sofern eine Auftragsverarbeitungs-Vereinbarung, die das gleiche Schutzniveau wie diese AV-V gewährleistet, mit dem Unterauftragnehmer abgeschlossen wurde, gestattet
(4) Eine Beauftragung von Unterauftragnehmern außerhalb der EU/des EWR ist nicht gestattet.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.
(6) Die Hinzuziehung weiterer oder ein Wechsel von Unterauftragnehmern ist erst nach Zustimmung des Auftraggebers zulässig und sofern das gleiche Schutzniveau vorliegt. Sofern bei Verweigerung der Zustimmung keine einvernehmliche Lösung gefunden werden kann, steht dem Auftraggeber ein außerordentliches Kündigungsrecht zu

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(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

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und 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.

Anlage 1: Allgemeine technische und organisatorische Maßnahmen nach nach Art. 32 EU-DSGVO

1. Zutrittskontrolle

Die Verarbeitung und Speicherung der Daten erfolgt ausschließlich auf dedizierten Servern, die bei der Hetzner Online GmbH gehostet werden.
Hetzner Online ist nach ISO/IEC 27001 zertifiziert.
Siehe: https://www.hetzner.de/unternehmen/zertifizierung/
Im Anhang: Zertifikat der Hetzner Online GmbH

2. Zugangskontrolle

Die Verarbeitung und Speicherung der Daten erfolgt ausschließlich auf dedizierten Servern, die bei der Hetzner Online GmbH gehostet werden.
Hetzner Online ist nach ISO/IEC 27001 zertifiziert.

Der Login auf die Server erfolgt ausschließlich über SSH Key-Based Authentication.
Sonstiger Zugriff auf den Server wird durch eine Software-Firewall unterbunden.

3. Zugriffskontrolle

Die Verarbeitung und Speicherung der Daten erfolgt ausschließlich auf dedizierten Servern, die bei der Hetzner Online GmbH gehostet werden.
Hetzner Online ist nach ISO/IEC 27001 zertifiziert.

Zugriff darauf haben nur berechtigte Personen der atenis GmbH.

Logins per SSH Key-Based Authentication werden protokolliert.

Die privaten SSH-Keys der berechtigten Mitarbeiter der atenis GmbH befinden sich auf den verschlüsselten Festplatten der Entwicklungsrechner. Die Zugänge zu den Rechnern sind mit Passwort und biometrischen Merkmalen gesichert. Auf den Entwicklungsrechner werden keine Kundendaten gespeichert.

4. Weitergabekontrolle

Die Verarbeitung und Speicherung der Daten erfolgt ausschließlich auf dedizierten Servern, die bei der Hetzner Online GmbH gehostet werden.
Hetzner Online ist nach ISO/IEC 27001 zertifiziert.

Für den administrativen Zugriff erfolgt der Zugriff ausschließlich über eine verschlüsselte SSH-Verbindung.

Der Zugriff über die Web-Schnittstelle ist ausschließlich verschlüsselt über HTTPS möglich („HTTPS-Only“).

Ein intrusion prevention System ist aktiv. Software-Aktualisierungen werden mindestens monatlich gepflegt . Die Server-Logfiles werden regelmäßig manuell gesichtet.

5. Eingabekontrolle

Protokollierung der Eingabe, Änderung und Löschung von Daten über die Web-Schnittstelle.

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen.

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

Eine 2-Faktor Authentifizierung ist obligatorisch.

6. Auftragskontrolle

Jeder der Vertragspartner verpflichtet die auf seiner Seite tätigen Personen gemäß § 5 Satz 2 BDSG schriftlich zum Datengeheimnis und weist dies dem Vertragspartner auf Anforderung nach.

7. Verfügbarkeitskontrolle

Datensicherungen werden automatisch einmal täglich durchgeführt, für 14 Tage aufbewahrt und danach gelöscht.

8. Trennungskontrolle

Im Datenbestand wird softwareseitig mit logischer Mandantentrennung gearbeitet.

Anlage 2: Zugelassene Subdienstleister

Subdienstleister für die Bereitstellung der Anwendung:

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen, Deutschland
Tel.: +49 (0)9831 505-0
E-Mail: info@hetzner.com

Die Datenverarbeitung und -speicherung erfolgt ausschließlich auf dedizierten Servern mit einem Serverstandort in Deutschland.

Anlage 3: Risikoeinstufung der KI-Funktion

1. Gegenstand und Zweck dieses Dokuments

Dieses Dokument dokumentiert die Einstufung der in zeufix integrierten KI-Funktion nach der Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-Verordnung). Es dient als dokumentierte Selbstbewertung des Anbieters im Sinne von **Artikel 6 Absatz 4 KI-VO** und stellt Betreibern (Schulen) auf Anfrage die Informationen bereit, die diese für ihre eigene Rechenschaftspflicht benötigen.

2. Beschreibung der KI-Funktion

Die KI-Funktion in zeufix unterstützt Lehrkräfte bei der sprachlichen Formulierung und Verbesserung von Texten für Zeugnisse und Lernentwicklungsberichte. Ihre Funktionsweise lässt sich wie folgt zusammenfassen:

- Die Lehrkraft gibt die pädagogische Bewertung inhaltlich selbst vor. Die KI unterstützt ausschließlich bei der Formulierung, Umformulierung und sprachlichen Glättung der Texte.
- Die KI trifft **keine** eigenständige Bewertung von Leistungen und **keine** Noten-, Versetzungs- oder Zulassungsentscheidungen.
- Die inhaltliche und rechtliche Letztverantwortung für jeden Text verbleibt vollständig bei der Lehrkraft. Jeder von der KI erzeugte oder überarbeitete Text wird von der Lehrkraft geprüft, bei Bedarf geändert und freigegeben.
- Der Betrieb erfolgt datenschutzkonform auf eigenen Servern. Es findet keine Weitergabe der Eingaben an Dritte statt.

3. Rechtlicher Rahmen

Die KI-Verordnung teilt KI-Systeme in Risikoklassen ein: verbotene Praktiken (Art. 5), Hochrisiko-Systeme (Art. 6 i. V. m. Anhang III), Systeme mit Transparenzpflichten (Art. 50) sowie Systeme mit minimalem Risiko.

Für den Bildungsbereich benennt **Anhang III Nummer 3** der KI-Verordnung insbesondere folgende Anwendungen als hochriskant: die Feststellung des Zugangs oder der Zulassung zu Bildungseinrichtungen (lit. a), die *Bewertung von Lernergebnissen* (lit. b), die Bewertung des angemessenen Bildungsniveaus (lit. c) sowie die Überwachung von Prüfungen (lit. d).

Nach **Artikel 6 Absatz 3 KI-VO** gilt ein in Anhang III genanntes System jedoch nicht als hochriskant, wenn es kein erhebliches Risiko für die Grundrechte birgt und lediglich eine eng begrenzte verfahrenstechnische, ergebnisverbessernde oder vorbereitende Aufgabe erfüllt. Diese Ausnahme greift nicht, wenn das System ein Profiling natürlicher Personen vornimmt.

4. Einstufung und Begründung

4.1 Prüfung von Anhang III Nr. 3 lit. b (Bewertung von Lernergebnissen)

Maßgeblich ist, ob die KI-Funktion eine Bewertung von Lernergebnissen vornimmt. Das ist nicht der Fall: Die inhaltliche Bewertung der Leistungen wird ausschließlich von der Lehrkraft vorgenommen. Die KI leistet einen sprachlichen Beitrag zu einem Text, dessen Bewertungsgehalt die Lehrkraft festgelegt hat. Sie ersetzt oder beeinflusst die pädagogische Bewertung nicht.

4.2 Prüfung der Ausnahme nach Art. 6 Abs. 3 KI-VO

Selbst wenn man die Zeugnistextunterstützung dem Umfeld von Anhang III Nr. 3 zuordnen wollte, erfüllt die KI-Funktion die Voraussetzungen der Ausnahme: Sie übernimmt eine unterstützende, ergebnisverbessernde bzw. vorbereitende Aufgabe zu einer Bewertung, die abschließend durch einen Menschen getroffen wird. Es findet kein Profiling von Schülerinnen und Schülern statt, das heißt keine automatisierte Auswertung personenbezogener Daten zur Bewertung persönlicher Aspekte. Die Bewertung selbst erfolgt durch die Lehrkraft.

4.3 Ergebnis

Nach dieser Bewertung ist die KI-Funktion in zeufix **kein Hochrisiko-KI-System** im Sinne von Artikel 6 in Verbindung mit Anhang III der KI-Verordnung. Sie ist als System mit begrenztem Risiko einzuordnen, für das die **Transparenzpflichten nach Artikel 50 KI-VO** maßgeblich sind.

5. Transparenzpflichten (Art. 50 KI-VO)

Die KI-Unterstützung ist innerhalb von zeufix als solche erkennbar. Die von der KI erzeugten oder überarbeiteten Texte werden von der Lehrkraft geprüft und verantwortet; die redaktionelle Verantwortung liegt damit bei einer natürlichen Person. Die Transparenzpflichten nach Artikel 50 gelten unabhängig von der Hochrisiko-Frage.

6. Zusammenfassung

- **Einstufung:** kein Hochrisiko-System; System mit begrenztem Risiko (Transparenzpflichten nach Art. 50 KI-VO).
- **Begründung:** Die KI unterstützt nur bei der sprachlichen Formulierung. Die Bewertung der Lernergebnisse und die Letztverantwortung verbleiben bei der Lehrkraft. Kein Profiling.
- **Betrieb:** datenschutzkonform auf eigenen Servern.

7. Hinweise und Vorbehalt

Dieses Dokument stellt die dokumentierte Selbstbewertung des Anbieters nach Art. 6 Abs. 4 KI-VO dar und ersetzt keine Rechtsberatung. Die endgültige rechtliche Verantwortung für die Einstufung trägt der Anbieter.

Die Schule ist als Betreiberin für die eigenen Pflichten verantwortlich, insbesondere für die menschliche Aufsicht, die zweckentsprechende Nutzung sowie die datenschutzrechtliche Information der betroffenen Personen nach DSGVO.

Die Anforderungen und Fristen der KI-Verordnung werden auf EU-Ebene fortlaufend konkretisiert. Diese Einstufung wird bei wesentlichen Änderungen der KI-Funktion oder der Rechtslage überprüft und aktualisiert.

CERTIFICATE

HETZNER

This is to certify that the Information Security Management System of

Hetzner Online GmbH
Industriestraße 25
D-91710 Gunzenhausen

with the scope

"The scope of application of the information security management system includes all hosting services and the data centers."

has been assessed and registered by SOCOTEC Certification Deutschland GmbH and found to be in compliance with the requirements of

ISO/IEC 27001:2022

This verification is subjected to the company maintaining its system to the required standard, which will be monitored by SOCOTEC Certification Deutschland GmbH. This certificate is valid for 3 years to satisfactory maintenance of the management system as per the standard.

Statement of Applicability(SoA):	Version 4.1 dated 09.07.2025
Day of Decision:	18.09.2025
Issued on:	18.09.2025
Validity certificate:	27.09.2025 - 26.09.2028
Certificate Number:	ZN-2025-35 V 1.1

SOCOTEC Certification
Deutschland GmbH
Graf-Dürkheim-Straße 3
87642 Halblech

Certification Body

DAkkS
Deutsche
Akkreditierungsstelle
D-ZM-18855-01-00

Vorlage 1.4

LOCATIONS

Location 1:

Hetzner Online GmbH
Sigmundstraße 135 90431
Nuremberg
Germany

Location 2:

Hetzner Online GmbH
Am Datacenter-Park 1 08223
Falkenstein/Vogtland
Germany

Location 3:

Hetzner Online GmbH
Huurrekuja 10
04360 Tuusula
Finland

Zur Ablage in Ihr Verzeichnis der Verarbeitungstätigkeiten:

Dokumentation der Verarbeitungstätigkeit zeufix.de / atenis GmbH

Angaben zum Verantwortlichen (hier Ihre Schuldaten eintragen)	
Verantwortlicher (gemäß Art. 4 Nr. 7 DSGVO)	
Gesetzlicher Vertreter	
Datenschutzbeauftragter (gemäß Art. 37 ff. DSGVO)	
Beschreibung der Verarbeitungstätigkeit	
Allgemeine Beschreibung der Verarbeitungstätigkeit	Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien) ◦ Personenstammdaten von Schülern (Name, Geburtsdatum, Geburtsort) ◦ Personenstammdaten von Lehrern (Name) ◦ Kommunikationsdaten (E-Mail) ◦ erfasste Schülerleistungen (Verbalbeurteilungen, Noten, sonst. Beurteilungen, Lernentwicklungsberichte)
Angaben zur Verarbeitungstätigkeit nach Maßgabe des Art. 30 Abs. 1 DSGVO	
Zwecke der Verarbeitung	Erstellung von Lernenwicklungsberichten, Zeugnissen, Abschlusszeugnissen. Notenverwaltung, Prüfungsorganisation Erstellung von Statistiken
Beschreibung der Kategorien betroffener Personen	Schulleitung, Mitarbeitende in der Schulverwaltung, Lehrkräfte, Schüler
Beschreibung der Kategorien personenbezogener Daten	Personenstammdaten von Schülern (Name, Geburtsdatum, Geburtsort) Personenstammdaten von Lehrern (Name) Kommunikationsdaten (E-Mail) erfasste Schülerleistungen (Verbalbeurteilungen, Noten, sonst. Beurteilungen, Lernentwicklungsberichte)
Empfänger oder Kategorien von Empfängern	
Interne Empfänger (innerhalb des Verantwortlichen)	Kundensupport, Buchhaltung, IT-Abteilung
Auftragsverarbeiter	atenis GmbH in 72116 Mössingen Die Verarbeitung und Speicherung der Daten erfolgt ausschließlich auf dedizierten Servern, die bei der Hetzner Online GmbH in Deutschland gehostet werden.
Datenweitergabe an Dritte	Keine

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	Keine
Drittstaaten / internationale Organisationen	Keine
Angemessenes Datenschutzniveau durch geeignete oder angemessene Garantie	-

Regelfristen für die Löschung der Daten	
Für die Löschung vorgesehene Fristen bzw. Speicherdauer oder Kriterien für deren Festlegung	s. Datenschutzerklärung auf login.zeufix.de

techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 DSGVO)	Die Verarbeitung und Speicherung der Daten erfolgt ausschließlich auf dedizierten Servern, die bei der Hetzner Online GmbH in Deutschland gehostet werden. Hetzner Online ist nach ISO/IEC 27001 zertifiziert. Der Login auf die Server erfolgt ausschließlich über SSH Key-Based Authentication. Zugriff darauf haben nur berechtigte Personen der atenis GmbH. Logins per SSH Key-Based Authentication werden protokolliert. Sonstiger Zugriff auf den Server wird durch eine Software-Firewall unterbunden. Der Zugriff über die Web-Schnittstelle ist ausschließlich verschlüsselt über HTTPS möglich („HTTPS-Only“). Protokollierung der Eingabe, Änderung und Löschung von Daten über die Web-Schnittstelle. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts. Eine 2-Faktor Authentifizierung ist obligatorisch. Datensicherungen werden automatisch einmal täglich durchgeführt, für 14 Tage aufbewahrt und danach gelöscht. Im Datenbestand wird softwareseitig mit logischer Mandantentrennung gearbeitet.

Datenschutzinformationen zur Nutzung von zeufix der atenis GmbH

Verantwortlicher und Datenschutzbeauftragter
(Art. 13 Abs. 1 lit. a) und b) DS-GVO)
Verantwortlicher gem. Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (EU-DS-GVO) ist:

Name und Adresse der Schule :	
Schulleitung:	
Telefon:	
E-Mail:	
Wir haben einen Datenschutzbeauftragten benannt. Diesen erreichen Sie unter:	
Telefon:	
E-Mail:	
	Kontakt des jeweiligen Schulamts oder RP oder der Schule sofern interner bDSB

Im Folgenden informieren wir über die Erhebung personenbezogener Daten bei Nutzung von zeufix der atenis GmbH. Personenbezogene Daten sind alle Daten, die auf Sie persönlich beziehbar sind, z. B. Name, Adresse, E-Mail-Adressen, Server-Logfiles.

Zwecke der Verarbeitung und Rechtsgrundlage (Art. 13 Abs. 1 lit. c) DS-GVO)

Wir verarbeiten personenbezogene Daten um Zeugnisnoten zu verwalten. Der Erziehungs- und Bildungsauftrag der Schule erfordert neben der Vermittlung von Kenntnissen, Fähigkeiten und Fertigkeiten auch deren Feststellung zur Kontrolle des Lernfortschritts zum Leistungsnachweis. Diese Leistungsnachweise sind von den Schulen zu erstellen und zu verarbeiten.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten in diesem Zusammenhang ist Art. 6 Abs. 1 lit. e) DSGVO (zur Erfüllung einer öffentlichen Aufgabe erforderlich) in Verbindung mit §§ 1 und 89 Abs. 1 Schulgesetz Baden-Württemberg sowie der Verordnung des Kultusministeriums über die Notenbildung (NVO).

Die Datenverarbeitung ist erforderlich.

Empfänger von personenbezogenen Daten (Art. 13 Abs. 1 lit. e) DS-GVO)

Gemäß Art. 4 Nr. 9 DSGVO werden als Empfänger nicht nur Dritte, sondern auch Auftragsverarbeiter erfasst. Die atenis GmbH bedient sich eines Unterauftragnehmers zum Speicherung der Daten (Hoster). Hierbei handelt es sich um sämtliche Daten, die in dem Zeugnisprogramm erfasst werden insbesondere Personenstammdaten von Schülern (Name, Geburtsdatum, Geburtsort), Personenstammdaten von Lehrern (Name), Kommunikationsdaten (E-Mail) erfasste Schülerleistungen (Verbalbeurteilungen, Noten,

sonst. Beurteilungen, Lernentwicklungsberichte). Beim Aufruf von zeufix werden darüber hinaus IP-Adresse und Server Logfiles sowie System- und Browsermerkmale verarbeitet.

Unser Hoster wird Ihre Daten nur insoweit verarbeiten, wie dies zur Erfüllung seiner Leistungspflichten erforderlich ist und unsere Weisungen in Bezug auf diese Daten befolgen.

Wir setzen folgende(n) Hoster ein:
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland
Als Standort der Server bei Hetzner verwenden wir Nürnberg oder Falkenstein.

Es besteht ein Vertrag über Auftragsverarbeitung (AVV) zwischen zeufix und dem oben genannten Anbieter. Hierbei handelt es sich um einen datenschutzrechtlich vorgeschriebenen Vertrag, der gewährleistet, dass dieser die personenbezogenen Daten unserer Webseitenbesucher nur nach unseren Weisungen und unter Einhaltung der DSGVO verarbeitet.

Drittlandtransfer (Art. 13 Abs. 1 lit. f) DS-GVO)

Bei der Nutzung dieser Webseite findet kein Datenexport in ein Drittland statt.

Informationen zu Cookies

Bei der Nutzung von zeufix wird ein technisch notwendiges Cookie gesetzt. Es handelt sich um ein Session-Cookie, welches nach Verlassen des Browsers gelöscht wird. Das Cookie ist technisch notwendig zur korrekten Anzeige des Programms sowie zur kurzzeitigen Speicherung der Zugangsdaten.

Speicherdauer (Art. 13 Abs. 2 lit. a) DS-GVO)

Die Daten werden von der atenis GmbH so lange gespeichert wie das Vertragsverhältnis zwischen ihr und der Schule besteht. Näheres regelt der Auftragsverarbeitungsvertrag. Die Schule ist verantwortlich für die Löschung entsprechend der Regelungen der Verwaltungsvorschrift Datenschutz an öffentlichen Schulen.

Die Server Logfiles werden werden von atenis 7 Tage gespeichert.

Ihre Rechte (Art. 13 Abs. 2 lit. b) und d) DS-GVO)

Sie haben gegenüber der Schule folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:

– Recht auf Auskunft,
– Recht auf Berichtigung oder Löschung,
– Recht auf Einschränkung der Verarbeitung,
– Recht auf Widerspruch gegen die Verarbeitung,
– Recht auf Datenübertragbarkeit.

Für die Rechte gelten die jeweiligen gesetzlichen Voraussetzungen.

Sie haben ferner das Recht sich bei der Datenschutzaufsichtsbehörde zu beschweren. Die zuständige Datenschutzaufsichtsbehörde ist:

(für Baden-Württemberg)
Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI)
Lautenschlagerstr. 20
70173 Stuttgart

(für Rheinland-Pfalz)
Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34
55116 Mainz