Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen der

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 § 9 BDSG und Anlage
- Zertifikat nach ISO/IEC 27001 der Hetzner Online GmbH

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).

(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 der Leistungsvereinbarung.

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.

i) 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.

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) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Eine Beauftragung von Unterauftragnehmern außerhalb der EU/des EWR ist nicht gestattet.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

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.

Allgemeine technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage

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.

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“).

5. Eingabekontrolle

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.

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 wird angeboten.

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

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.

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

8. Trennungskontrolle

Im Datenbestand wird softwareseitig mit logischer Mandantentrennung gearbeitet.

FOX Certification

ZERTIFIKAT

FOX Certification GmbH bescheinigt hiermit, dass das Informationssicherheitsmanagementsystem des Antragstellers

HETZNER

an den Standorten Nürnberg und Falkenstein/Vogtland:

Hetzner Online GmbH
Sigmundstraße 135
90431 Nürnberg

Hetzner Online GmbH
Am Datacenter-Park
08223 Falkenstein/Vogtland

mit dem Geltungsbereich

"Der Anwendungsbereich des Informationssicherheits-Managementsystems umfasst die Infrastruktur, den Betrieb und Kundensupport der Rechenzentren"

auf Grundlage des Statement of Applicability in der Version 3.0 die Anforderungen des folgenden Regelwerks erfüllt:

ISO/IEC 27001:2013

Im Zertifizierungsaudit konnten Nachweise vorgelegt werden, die die Erfüllung der Anforderungen belegten.

Statement of Applicability(SoA):	Version 3.0
Gültigkeit Zertifikat:	27.09.2019 - 26.09.2022
Zertifikatsnummer:	ZN-2019-11

FOX Certification GmbH
Graf-Dürkheim-Straße 3
87642 Halblech

Aykut Bader, Geschäftsführer

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

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
Beschreibung der Kategorien betroffener Personen	Lehrer 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.