Datenschutzvereinbarung Bereitstellung des digitalen Lernangebotes Deutschfuchs

---

zwischen

Deutschfuchs Testschule

Musterstraße 12
12345 Musterstadt
Deutschland

DFID: 4170

- Auftraggeber -

und

Deutschfuchs Gesellschaft für digitalen Unterricht mbH
Weyerstr. 29-31
50676 Köln

- Auftragnehmer -

Erstellt und unterzeichnet vom Auftragnehmer

Köln, den 18.12.2023.

Bitte unterschreiben Sie auf Seite 7 und senden uns den Vertrag per E-Mail (info@deutschfuchs.de), Fax (0221-29249541) oder Briefpost zurück.

Präambel

Zwischen den Parteien besteht ein Vertragsverhältnis über die Bereitstellung von Software in einem Rechenzentrum („SaaS“).

Diese Vereinbarung wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Regelungen des Art. 28 der Datenschutz-Grundverordnung (DSGVO) zwischen den Parteien getroffen.

1. Allgemeines

Der Auftragnehmer stellt für den Auftraggeber die Software „Deutschfuchs“ (digitales Lehrwerk für Deutsch als Fremdsprache mit Schülerverwaltung und Selbstlernbereich) im Rahmen eines SaaS (Software as a Service)-Modells über einen Webserver (Hosting) bereit und berät den Auftraggeber hinsichtlich seiner IT-Anlage, benötigter Hardware und der Verwendung von Software und digitalen Lernangeboten im Bildungsbereich (IT-Beratung). In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer personenbezogene Daten verarbeitet, um diesen Aufgaben nachkommen zu können. Die Verarbeitung erfolgt in diesem Fall ausschließlich innerhalb der EU. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich nach dokumentierten Weisungen des Verantwortlichen. Weisungen sind grundsätzlich schriftlich zu erteilen. Mündlich erteilte Weisungen müssen unverzüglich schriftlich bestätigt werden.

2. Dauer und Beendigung des Auftrags

(1) Der Auftragnehmer führt für den Auftraggeber Leistungen (Bereitstellung der Software „Deutschfuchs“ in einem Rechenzentrum [„SaaS“] und Beratung zu den in Punkt 1 genannten Themen sowie allgemeinen Bildungsthemen) durch. Zwischen den Parteien besteht diesbezüglich ein Vertragsverhältnis („Hauptvertrag“), das entweder auf individuellen vertraglichen Vereinbarungen, allgemeinen Geschäftsbedingungen oder auf gesetzlichen Regelungen (z.B. BGB) basiert. Diese Vereinbarung beginnt ab Unterzeichnung durch beide Parteien und gilt für die Dauer des jeweiligen Hauptvertrages.

(2) Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

3. Gegenstand des Auftrags

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

- Bereitstellung einer Software („Deutschfuchs“) in einem Rechenzentrum („SaaS“).
- Veröffentlichung von Unterrichtsmaterialien, Aufgaben, Vokabeln, Spielen und weiteren digitalen Lernangeboten über diese Software.
- Verwaltung der Personen mit Zugriffsrechten, dies umfasst zwei Gruppen: 1) Lehrkräfte, die über einen personalisierten Zugang verfügen. Diese können Unterrichtsmaterial downloaden und für Schüler freigeben, Schülerzugänge erzeugen, ändern und löschen und alle sonstigen Angebote der Software „Deutschfuchs“ nutzen. 2) Schüler, die von ihrer zuständigen Lehrkraft einen Zugang erhalten.
- Fernwartung von IT-Systemen.

Im Zuge der Leistungserbringung zum Zwecke der Softwarebereitstellung kann ein Zugriff auf personenbezogene Daten durch den Auftragnehmer nicht ausgeschlossen werden, zum Beispiel bei konkreten Fragen zur Nutzung der Software, beim Import von Daten und bei der Schulung von Kolleg*innen im Produktivbetrieb. Folgende Datenarten sind daher regelmäßig Gegenstand der Verarbeitung:

- Vorname, Nachname und E-Mail-Adresse der Personengruppe „Lehrkräfte“. Diese Daten sind notwendig, um die Software benutzen zu können.
- Ein Name (Pseudonym, Vorname, Nachname oder eine Kombination daraus) für die Personengruppe „Schüler“.
- Für die Personengruppe Schüler weiterhin: Ein Passwort, welches von allen befugten Lehrkräften eingesehen und geändert werden kann, ein zufällig generierter und gleichbleibender Zugangscode, der zum Login benötigt wird, verschiedene Detaildaten zum Lernfortschritt des Schülers (z.B. Sprache der Übersetzungen, freigeschaltete Zeiten, Punktestände bei Spielen) und alle Daten, die der Schüler über einen Zugang in das System eingibt. Das sind typischerweise die Lösungen für gestellte Aufgaben (z.B. Einsetzübungen, Lückentexte, Multiple-Choice-Fragen) und Texte, die in einem Freitext-Editor eingegeben, angezeigt und gespeichert werden können. Jegliche Eingaben, die die Personengruppe „Schüler“ tätigt, können von allen Mitgliedern der Personengruppe „Lehrkräfte“ innerhalb der Organisation des Auftraggebers eingesehen und verändert werden.

Kreis der von der Datenverarbeitung Betroffenen:

- Beschäftigte des Auftraggebers („Lehrkräfte“)
- Kunden des Auftraggebers („Schüler“)

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Bereitstellung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Wartung und Pflege durch den Auftragnehmer feststellt.

5. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Zusammenhang mit den Wartungs-/Pflegearbeiten im Auftrag verarbeitet, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(3) Auftragnehmer verpflichtet sich, den Auftraggeber zu informieren, falls er durch nationales oder europäisches Recht zur Verarbeitung der im Rahmen dieses Vertrags überlassenen personenbezogenen Daten verpflichtet wird, es sei denn, das betreffende Recht untersagt eine solche Information aus wichtigen Gründen des öffentlichen Interesses

(4) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(5) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO im Falle einer Datenschutzverletzung bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere und unverzüglich über unbefugte Zugriffe auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, informieren.

(6) Der Auftragnehmer wird seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nachkommen.

6. Kontrollbefugnisse

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

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

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden könnten.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO i.V.m. § 40 BDSG, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten, die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

7. Fernwartung

Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

8. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **ANLAGE 2** zu diesem Vertrag angeben.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, ob dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten benannt hat, sofern dies nach Art. 37 DSGVO i.V.m. § 38 BDSG erforderlich ist.

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

(4) Die Verpflichtung des Unterauftragnehmers muss den Anforderungen von Art. 28 Abs. 4 DSGVO entsprechen.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(6) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

9. Vertraulichkeit und Geheimhaltung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Dies gilt insbesondere in den Fällen, in denen der Auftraggeber zur Einhaltung der Schweigepflicht aus § 203 StGB verpflichtet ist. Der Auftraggeber wird dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese zur Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet hat, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

10. Wahrung von Betroffenenrechten und Unterstützungspflichten

Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer unterstützt den Auftraggeber jedoch bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten zum Schutz personenbezogener Daten. Hierzu gehören u.a.
(1) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
(2) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen zur Verfügung zu stellen
(3) die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgenabschätzung
(4) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

11. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen.

(2) Bei Bereitstellung der Software in einem Rechenzentrum („SaaS“) gelten neben den technischen und organisatorischen Maßnahmen des Auftragnehmers **(ANLAGE 1)** auch die technischen und organisatorischen Maßnahmen des Betreibers des Rechenzentrums. Diese sind diesem Vertrag gesondert beigefügt. **(ANLAGE 2 Fa. Hetzner)**

(3) Die Speicherung der Daten bei Bereitstellung von Software in einem Rechenzentrum („SaaS“) erfolgt aktuell ausschließlich in den Rechenzentren der Firmen Hetzner Online GmbH, Mittwald CM Service GmbH & Co. KG und Strato Online AG. Für Mitarbeiter des Auftragnehmers besteht eine Zugriffsmöglichkeit auch außerhalb der Geschäftsräume des Auftragnehmers. Ein Zugriff außerhalb der Geschäftsräume erfolgt allerdings nur, wenn die örtlichen Gegebenheiten vor Ort die Datenschutzrechte aller betroffenen Personen berücksichtigen. Der Zugriff erfolgt verschlüsselt und erst nach Authentifizierung. Einer Speicherung in weiteren Rechenzentren wird zugestimmt, wenn der Standort des Rechenzentrums in Deutschland liegt und dieses Rechenzentrum über ein gleichwertiges oder höheres Schutzniveau als ISO 27001 verfügt.

(4) Für den Fall, dass der Auftragnehmer die Wartung und Pflege von IT-Systemen für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt (z.B. im Falle der Fernwartung), sind vom Auftragnehmer zwingend die in der **ANLAGE 1** zu diesem Vertrag genannten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten einzuhalten.

(5) Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforder-

lich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

12. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

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

13. Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____, den _____

Ort Datum

_____

- Stempel / Unterschrift Auftraggeber -

Anlagen:

- Anlage 1: Technische und organisatorische Maßnahmen
- Anlage 2: Unterauftragnehmer
- Anlage 3: Weitergehende Informationen zur Programmarchitektur
- Anlage 2 der Firma Hetzner (TOM)

Anlage 1:
Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

Der Auftragnehmer ist verpflichtet, nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO einzuhalten:

1. Vertraulichkeit

Zutrittskontrolle
Der Auftragnehmer trägt Sorge dafür, dass seine Büro- und Geschäftsräume grundsätzlich außerhalb der Büro- und Geschäftszeiten geschlossen sind.

Während der Büro- und Geschäftszeiten ist sichergestellt, dass Besucher oder sonstige Dritte sich nicht alleine in Räumen bewegen können, in denen sie Zugang zu personenbezogenen Daten erhalten könnten.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgen nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zugangskontrolle
Um Zugang zu IT-Systemen zu erhalten, müssen der Auftragnehmer und seine Beschäftigten über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von einem oder mehreren Administratoren vergeben.

Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 10 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte Verbindungen.

Alle Server und Client-Systeme, die bei der Erbringung von Leistungen für den Auftraggeber im Einsatz sind, sind durch Firewalls geschützt, die gewartet und mit aktuellen Updates und Patches versorgt werden.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter, die der Auftragnehmer vom Auftraggeber erhält oder für dessen IT-Systeme verwendet, werden grundsätzlich verschlüsselt gespeichert und sind nur den Beschäftigten zugänglich zu machen, die konkret mit der Erbringung von Leistungen für den Auftraggeber betraut sind.

Zugriffskontrolle
Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte

auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Trennung
Soweit der Auftragnehmer personenbezogene Daten vom Auftraggeber im Zusammenhang mit der Auftragsverarbeitung erhält, wird er diese getrennt von Daten anderer Kunden verarbeiten.

Pseudonymisierung & Verschlüsselung
Ein administrativer Zugriff auf IT-Systeme des Auftraggebers erfolgt grundsätzlich über verschlüsselte Verbindungen, soweit dieser nicht innerhalb der Räumlichkeiten des Auftraggebers erfolgt.

2. Integrität

Eingabekontrolle
Der Auftragnehmer wird Eingaben, Änderungen oder Löschungen von personenbezogenen Daten, die er im Auftrag des Auftraggebers durchführt, in geeigneter Weise dokumentieren, sofern nicht sichergestellt ist, dass das jeweilige IT-System selbst eine Protokollierung entsprechender Aktivitäten durchführt.

Weitergabekontrolle
Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang erfolgen, wie und soweit dies mit dem Auftraggeber abgestimmt ist.

Die Nutzung von privaten Datenträgern ist dem Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung für den Auftraggeber untersagt.

3. Verfügbarkeit und Belastbarkeit
Soweit der Auftragnehmer personenbezogene Daten oder Zugangsdaten für den Auftraggeber speichert oder verwaltet, trägt er Sorge dafür, dass diese Daten mindestens täglich inkrementell und wöchentlich „voll“ gesichert werden. Es gibt ein Datensicherungskonzept, das auch das erfolgreiche Testen der Wiederherstellung von Daten beinhaltet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Beschäftigten dazu bei, dass eine Verarbeitung personenbezogener Daten in einer Weise gewährleistet ist, die den Anforderungen der DSGVO entspricht.

Dies beinhaltet insbesondere eine regelmäßige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich dem Auftraggeber gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsverarbeitung für den Auftraggeber verarbeitet werden.

Auftragskontrolle
Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Unterauftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
Etwaige nach Art. 25 DSGVO erforderliche Maßnahmen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten durch den Auftraggeber sind vom Auftraggeber zu treffen bzw. durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer festzulegen.

Anlage 2:
Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

Name	Anschrift	Kontakt	Leistung
Aschemeier Beratungsgesellschaft mbH	Schillerstr. 10a 33609 Bielefeld	**T** 0521-25670070 www.aschemeier.net	Softwareentwicklung Technischer Support
Mittwald CM Service GmbH & Co. KG	Königsberger Straße 4-6 32339 Espelkamp	**T** 05772-293100 www.mittwald.de	Hosting und Wartung der Server zur Bereitstellung von Software im SaaS-Modell
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	**T** 09831-5050 www.hetzner.de	Hosting und Wartung der Server zur Bereitstellung von Software im SaaS-Modell
Weber eBusiness Services GmbH	Bahnhofstraße 16 72336 Balingen	**T** 0800-2608000 www.weber.cloud	Zum 01.01.2023 entfallen
STRATO AG	Pascalstraße 10 10587 Berlin	**T** 030-3001460 www.strato.de	Bereitstellung von Speicherkapazität für Backups
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen	**T** 07161-305897897 www.teamviewer.com	Software zur Fernwartung / Fernsteuerung von Computern
Liersch & Rische GbR	Schillerstr. 10a 33609 Bielefeld	**T** 0521-89732205 www.hsm-support.de	Technische Betreuung, IT-Service
Digistore 24 GmbH	St.-Godehard-Straße 32 31139 Hildesheim	**T** 05121-9288860 https://www.digistore24.com/	Zahlungsabwicklung bei Onlinebestellungen / Onlinezahlungen.
Hueber Verlag GmbH & Co KG	Bauberger-straße 30 80992 München	**T** 089-96020 www.hueber.de	Vertrieb, Marketing und Bearbeitung von Kundendienstanfragen

Anlage 3:
Allgemeine Informationen und Funktionen zur Sicherstellung der Datensicherheit und Integrität in der Software „Deutschfuchs“

Die Deutschfuchs Gesellschaft für digitalen Unterricht mbH stellt ihre Softwarelösungen auf Basis einer selbst entwickelten Plattform bereit. Die nachfolgenden Informationen gelten für den internen, registrierungs- und kostenpflichtigen Bereich von Deutschfuchs („nach dem Login“).

Bereits bei der Entwicklung dieser Plattform haben wir uns besonders auf den Schutz Ihrer Daten fokussiert und eine Reihe von Maßnahmen ergriffen, die dem Prinzip „Privacy by Default“ der Europäischen Datenschutz-Grundverordnung folgen. Im Folgenden finden Sie eine nicht abschließende, ständig erweiterte Auflistung unserer Maßnahmen:

Datenschutz / allgemeine Sicherheit

- Wir verzichten vollständig auf die Integration von ständig aktiven Programmbibliotheken, die über ein CDN (Content-Delivery-Network) oder eine Cloudschnittstelle angeboten werden. Alle Bestandteile der Software sind ausschließlich auf unseren Servern in einem zertifizierten deutschen Rechenzentrum gespeichert.
- Es erfolgt keine Weitergabe der Daten zu Analyse oder Auswertungszwecken an Dritte (z.B. kein Einsatz von Google Analytics).
- Die Benutzeranmeldung (Personengruppe Lehrkräfte) erfolgt mit Anmeldename sowie Kennwort und wird nach 20 Fehlversuchen gesperrt. Die erneute Freigabe ist nur über unseren Support möglich.
- Einige Aktionen innerhalb der Software (Anmeldung, fehlgeschlagene Anmeldung, Ändern der Einstellungen, Erzeugen und Löschen von Schülerzugängen) werden unwiderruflich mit einem Zeitstempel und dem ausführenden Nutzer protokolliert.
- Der Zugriff auf unsere Systeme ist ausschließlich verschlüsselt möglich. (TLS-Verschlüsselung ab Version 1.2, 256-bit-Schlüssel). Unverschlüsselte Verbindungen werden nicht akzeptiert.
- Die internen Passwörter für den Zugriff auf Verwaltungsinstrumente, FTP-Server, Datenbankserver etc. werden regelmäßig geändert und sind mindestens 14 Zeichen (inkl. Sonderzeichen) lang.
- Die Verarbeitung von personenbezogenen Daten findet ausschließlich auf Servern in zertifizierten Rechenzentren in Deutschland statt. Aktuelle Protokolle anerkannter Prüforganisationen über die Einhaltung der Sicherheitsmaßnahmen in diesen Rechenzentren sind auf Anfrage erhältlich.
- Neue, optionale Technologien (KI, LLM, Sprachsynthese und -analyse) können auf Diensten von US-Konzernen basieren. Diese Dienste sind gesondert gekennzeichnet. Der Aufruf dieser Funktionen erfolgt nicht direkt durch den Auftraggeber, sondern immer über den Umweg über unsere deutschen Server. Eine Verarbeitung von personenbezogenen Daten ist somit ausgeschlossen, sofern der Auftragnehmer etwaige Eingabefelder nicht bewusst und entgegen unserer Anweisung mit persönlichen Informationen befüllt.

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

- **Zutrittskonstrolle**
  - **Datacenter-Parks in Nürnberg, Falkenstein und Helsinki**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenter-Park
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
  - **Verwaltung**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Videoüberwachung an den Ein- und Ausgängen
- **Zugangskontrolle**
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
    - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem

Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.

- für Managed Server, Webhosting und Storage Share
    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

- **Zugriffskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
    - für Managed Server, Webhosting und Storage Share
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
        - Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.
- **Datenträgerkontrolle**
    - **Datacenter-Parks in Nürnberg, Falkenstein und Helsinki**
        - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
        - Defekte Festplatten, die nicht sicher gelöscht werden können,

werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).

- **Trennungskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
    - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Trennungskontrolle obliegt dem Auftraggeber.
  - für Managed Server, Webhosting und Storage Share
    - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
    - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- **Pseudonymisierung**
  - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
  - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
  - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- **Eingabekontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

- für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
- für Managed Server, Webhosting und Storage Share
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
        - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
        - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
        - Monitoring aller relevanten Server.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Dauerhaft aktiver DDoS-Schutz.
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Datensicherung obliegt dem Auftraggeber.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Dauerhaft aktiver DDoS-Schutz.
    - Für Managed Server, Webhosting und Storage Share
        - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
        - Einsatz von Festplattenspiegelung.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Einsatz von Softwarefirewall und Portreglementierungen.

- Dauerhaft aktiver DdoS-Schutz.

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**
  - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- **Auftragskontrolle**
  - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
  - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
  - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.