Vereinbarung zur Auftragsverarbeitung
gemäß Art. 28, 29 EU-DSGVO

Zwischen

***
***
***

(Verantwortlicher, nachfolgend „**Auftraggeber**“ genannt)

und

Terra Infinity UG
Adams-Lehmann-Str. 60
80797 München

(Auftragsverarbeiter, nachfolgend „**Auftragnehmer**“ genannt)

– beide Vertragsparteien nachfolgend auch einzeln **Partei** und gemeinsam **Parteien** genannt –

1 Anwendungsbereich

1.1 Im Rahmen der Leistungserbringung nach dem Hauptvertrag vom [Datum] samt seinen Anlagen (nachfolgend einheitlich „Vertrag“ genannt) ist es erforderlich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers oder sonstiger Dritter (nachfolgend einheitlich „Kundendaten“ genannt) erhält.

1.2 Alle Begrifflichkeiten dieser Vereinbarung zur Auftragsverarbeitung werden im Sinn und dem Verständnis nach der europäischen Datenschutzgrundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates) verwendet.

1.3 Im Falle eines Widerspruchs zwischen den Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung und denjenigen des Vertrags gehen die Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung denjenigen des Vertrages vor.

2 Auftragsverarbeitung

2.1 Der Auftragnehmer verarbeitet die Kundendaten ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 28, 29 EU-DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn Verantwortlicher („Herr der Daten“) und ist für die Rechtmäßigkeit der auftragsgemäßen Verarbeitung der Kundendaten verantwortlich.

2.2 Die Verarbeitung der Kundendaten hat ausschließlich und vollständig in der/dem in Anlage 1 dieser Vereinbarung zur Auftragsverarbeitung abschließend festgelegten Art und Zweck zu erfolgen. Die Verarbeitung der Kundendaten umfasst die in Anlage 1 dieser Vereinbarung zur Auftragsverarbeitung abschließend festgelegte Art der Kundendaten und den dort festgelegten Kategorien der durch die Verarbeitung betroffenen Personen.

2.3 Der Auftragnehmer erwirbt an den Kundendaten keine Rechte und ist auf Verlangen des Auftraggebers jederzeit zur Herausgabe der Kundendaten verpflichtet. Zurückbehaltungsrechte in Bezug auf die Kundendaten sind ausgeschlossen. Der Auftragnehmer ist verpflichtet, auf Weisung des Auftraggebers Kundendaten zu berichtigen oder deren Verarbeitung einzuschränken.

2.4 Der Auftragnehmer ist verpflichtet, den ersteilten Weisungen des Auftraggebers zur Verarbeitung der Kundendaten (nachfolgend einheitlich „Weisungen" genannt) uneingeschränkt zu folgen. Im Einzelfall erteilte Weisungen haben schriftlich oder per E-Mail zu erfolgen. In begründeten Einzelfällen können Weisungen auch mündlich erteilt werden, müssen dann aber vom Auftraggeber zeitnah schriftlich oder per E-Mail bestätigt werden. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen gesetzliche Vorschriften und/oder den Vertrag verstößt, so ist der Auftragnehmer verpflichtet, den Auftraggeber hierauf unverzüglich hinzuweisen, sowie berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

2.5 Der Auftragnehmer ist verpflichtet, einen betrieblichen Datenschutzbeauftragten schriftlich zu bestellen, soweit er in der Regel mindestens zwanzig (20) Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 S. 1 BDSG). Der betriebliche Datenschutzbeauftragte des Auftragnehmers ist dem Auftraggeber schriftlich zu benennen. Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten wird dem Auftraggeber durch den Auftragnehmer unverzüglich schriftlich mitgeteilt.

3 Datensicherheit / Technische und organisatorische Maßnahmen

3.1 Der Auftragnehmer hat gemäß Art. 28 Abs. 3 S. 2 lit. b, 29 und 32 Abs. 4 EU-DSGVO die bei der Verarbeitung von Kundendaten beschäftigten Personen zur Vertraulichkeit zu verpflichten.

3.2 Der Auftragnehmer ist verpflichtet, die Organisation der von ihm zu verantwortenden Prozesse und Maßnahmen derart zu gestalten, dass sie den Anforderungen des Datenschutzes gerecht werden und dass sichergestellt ist, dass Kundendaten nur entsprechend der durch den Auftraggeber erteilten Weisungen verarbeitet werden (insbesondere durch die Trennung der Kundendaten von Daten anderer Auftraggeber des Auftragnehmers) und nicht unbefugt Dritten zur Kenntnis gelangen können.

3.3 Der Auftragnehmer ist verpflichtet, innerhalb und im Rahmen des ihm nach dem Vertrag zugewiesenen Verantwortungsbereichs die Sicherheit der Verarbeitung gemäß Art. 28 Abs. 3 lit. c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO einzuhalten. Er ist verpflichtet geeignete technische und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um Datensicherheit und Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und der Zweck der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen. Vorbehaltlich weiterer Weisungen des Auftraggebers gelten mit Abschluss des Vertrages und/oder dieser Vereinbarung zur Auftragsverarbeitung, die in Anlage 2 dieser Vereinbarung zur Auftragsverarbeitung benannten technischen und organisatorischen Maßnahmen als Maßnahmen im Sinne dieser Ziffer 3.3 dieser Vereinbarung zur Auftragsverarbeitung.

3.4 Der Auftragnehmer ist verpflichtet, keine Kundendaten über das zur Erfüllung der Verpflichtungen aus dem Vertrag unbedingt erforderliche Maß hinaus zu verarbeiten (insbesondere nicht unbefugt zu vervielfältigen oder unbefugt an Dritte weiterzugeben).

3.5 Der Auftragnehmer hat ihm überlassene und alle ergänzend verarbeiteten Kundendaten unwiderruflich in allen Systemen des Auftragnehmers (einschließlich sämtlicher Vervielfältigungen, auch in Archivierungs- und Sicherungsdateien) nach Maßgabe der Bestimmungen der Anlage 2 dieser Vereinbarung zur Auftragsverarbeitung zu löschen oder zu vernichten (nachfolgend einheitlich „löschen" genannt), sobald die Verarbeitung der Kundendaten nicht mehr für die Erfüllung des Zwecks der Auftragsverarbeitung erforderlich ist (regelmäßig bei Beendigung des Vertrages).

3.6 Die Löschung von Kundendaten ist durch den Auftragnehmer zu dokumentieren und dem Auftraggeber gegenüber auf Anfrage schriftlich zu bestätigen. Nicht von dieser Löschpflicht erfasst werden Kundendaten, die aufgrund einer gesetzlichen Aufbewahrungs- und/oder Speicherpflicht aufzubewahren sind. Diese Kundendaten sind nach den gesetzlichen Bestimmungen in ihrer Verarbeitung einzuschränken und mit Ablauf der Aufbewahrungs- und/oder Speicherpflicht zu löschen.

4 Meldepflicht

Im Falle von in Art. 33 und 34 EU-DSGVO bestimmten Ereignissen sowie bei Verstößen des Auftragnehmers oder der beim Auftragnehmer beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder die in dieser Vereinbarung zur Auftragsverarbeitung nebst ihren Anhängen getroffenen Bestimmungen ist der Auftragnehmer verpflichtet, unverzüglich sämtliche erforderlichen Maßnahmen einzuleiten, um entstandene Gefährdungen für die Integrität und Vertraulichkeit der Kundendaten auszuschließen. Weiterhin ist der Auftragnehmer in diesen Fällen verpflichtet, dem Auftraggeber sowie dem Datenschutzbeauftragten des Auftraggebers unverzüglich die konkreten Umstände unter Angabe von Ursachen, den genauen Zeitpunkt sowie das Ausmaß des Ereignisses zu melden und die weitere Verarbeitung der Kundendaten mit dem Auftraggeber abzustimmen.

5 Unterauftragnehmer

5.1 Der Auftragnehmer ist berechtigt, Unterauftragnehmer mit der Erfüllung seiner Verpflichtungen zu beauftragen, nachdem der Auftragnehmer den Unterauftragnehmer derart schriftlich verpflichtet hat, wie der Auftragnehmer aufgrund dieser Vereinbarung zur Auftragsverarbeitung gegenüber dem Auftraggeber verpflichtet ist. Der Auftragnehmer hat den Unterauftragnehmer dabei insbesondere so zu verpflichten, dass der Auftraggeber seine in Ziffer 7 dieser Vereinbarung zur Auftragsverarbeitung festgelegten Kontrollrechte auch unmittelbar gegenüber dem Unterauftragnehmer geltend machen kann. Als Unterauftragnehmer im Sinne dieser Ziffer 5 gelten nicht mit dem Auftragnehmer arbeitsvertraglich verbundene oder im Rahmen der Arbeitnehmerüberlassung entliehene und bei der Verarbeitung von Kundendaten beschäftigte Personen, die unter Beachtung von Ziffer 3.1 dieser Vereinbarung zur Auftragsverarbeitung nachweislich verpflichtet wurden.

5.2 Der Auftragnehmer hat zum Abschluss des Vertrags die in Anlage 3 dieser Vereinbarung zur Auftragsverarbeitung aufgelisteten Unterauftragnehmer mit der Erfüllung seiner Verpflichtungen beauftragt.

5.3 Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

6 Anfragen Dritter, Kontrollen durch Aufsichtsbehörden

6.1 Soweit der Auftragnehmer Anfragen Dritter (insbesondere von betroffenen Personen und Journalisten) zur Auskunft über die Verarbeitung von Kundendaten oder Ereignisse, welche die Meldepflicht nach Ziffer 4 dieser Vereinbarung zur Auftragsverarbeitung auslösen, erhält, ist der Auftragnehmer verpflichtet, den Auftraggeber und den Datenschutzbeauftragten des Auftraggebers unverzüglich über die Anfrage zu informieren. Der Auftragnehmer hat es zu unterlassen, Dritten Auskünfte nach Satz 1 dieser Ziffer 6.1 zu erteilen, es sei denn, er ist gesetzlich zur Erteilung einer solchen Auskunft verpflichtet. Ziffer 6.1 dieser Vereinbarung zur Auftragsverarbeitung gilt entsprechend, soweit Aufsichtsbehörden beim Auftragnehmer Kontrollen ankündigen oder unangekündigt durchführen.

6.2 Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

7 Kontroll- und Auskunftsrechte

Der Datenschutzbeauftragte des Auftraggebers und/oder von diesem beauftragte Dritte haben jederzeit das Recht, nach angemessener schriftlicher Vorankündigung, die Geschäftsräume des Auftragnehmers zu betreten, um sich zeitlich und räumlich uneingeschränkt von der Einhaltung der einschlägigen gesetzlichen und vertraglichen Datenschutzbestimmungen zu überzeugen. Der Auftragnehmer gewährt dem Datenschutzbeauftragten des Auftraggebers und/oder von diesem beauftragten Dritten in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte. Gleiches gilt für die für den Auftraggeber zuständige(n) Aufsichtsbehörde(n).

8 Unterstützung des Auftraggebers

8.1 Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 16 - 21 EU-DSGVO genannten Rechte von betroffenen Personen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich auf Anfrage zur Verfügung zu stellen.

8.2 Der Auftragnehmer ist weiterhin verpflichtet, den Auftraggeber bei der Durchführung von Datenschutz-Folgeabschätzungen gemäß Art. 35 EU-DSGVO sowie im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde gemäß Art. 36 EU-DSGVO auf schriftliche Anfrage zu unterstützen.

8.3 Der Auftragnehmer ist verpflichtet, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der in Art. 28 EU-DSGVO niedergelegten Pflichten zu überlassen.

9 Schlussbestimmungen

Soweit zwischen den Vertragsparteien nichts anderes ausdrücklich vereinbart ist, richtet sich die Dauer der Datenverarbeitung im Auftrag nach den Bestimmungen zur Laufzeit des Vertrags.

Anlage 1: Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie Art der Daten und Kategorien betroffener Personen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Beauftragte Unterauftragnehmer

Ort, Datum:	Ort, Datum:
_____	_____
Für den Auftraggeber:	Für den Auftragnehmer
_____	_____

Anlage 1 zur Vereinbarung zur Auftragsverarbeitung: Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie Art der Daten und Kategorien betroffener Personen

1 Gegenstand, Art und Zweck der Auftragsverarbeitung

Die vom Auftragnehmer entwickelte Online-Lernplattform „eStudy.fm“ bietet alle Funktionen an, welche für die Durchführung eines zum Präsenzunterricht gleichwertigen webbasierten Distanzunterrichts notwendig sind. Lehrkräfte können dabei die Online-Lernplattform „eStudy.fm" sowohl für einen reinen Distanzunterricht einsetzen, als auch begleitend zum Präsenzunterricht (bspw. im Rahmen der direkten Kommunikation mit einzelnen Schülern oder auch deren Eltern) nutzen.

Dabei können Lehrkräfte ihren Schülern über die Online-Lernplattform „eStudy.fm“ Aufgaben in Form von Tickets einstellen und diese nach Bearbeitung durch die Schüler in der Online-Lernplattform „eStudy.fm“ dort bewerten. Daneben können Lehrkräfte Unterrichtsstunden über integrierte Videokonferenzen- und Whiteboardfunktionen durchführen und mit ihren Schülern per Chat und Push-Nachrichten kommunizieren.

Gegenstand, Art und Zweck der Auftragsverarbeitung ist die Bereitstellung der Online-Lernplattform „eStudy.fm“ sowie die ergänzende Pflege und Wartung der Online-Lernplattform „eStudy.fm“ durch den Auftragnehmer.

2 Dauer der Auftragsverarbeitung

Die für die Bereitstellung der Lernplattform „eStudy.fm“ gegenständliche Vereinbarung zur Auftragsverarbeitung wird auf unbestimmte Zeit geschlossen und endet automatisch mit der Laufzeit des letzten zwischen den Parteien geschlossenen Vertrags.

3 Art der Daten, die der Auftragnehmer verarbeitet

Durch den Auftragnehmer können Kontaktdaten, Kommunikationsdaten, Bewertungen und Noten sowie alle sonstige personenbezogenen Daten, welche Benutzer in der Lernplattform „eStudy.fm“ hochladen, verarbeitet werden. Dies sind üblicherweise die folgenden personenbezogenen Daten:

- Name, Vorname, ggf. E-Mail-Adresse, ggf. Foto,
- Bild und Ton,
- Kommunikationsdaten, insbesondere Nachrichten zwischen Benutzern, Chat-Diskussionen und Kommentare,
- Bewertungen, Bewertungsergebnisse sowie Noten,
- Kalendereinträge,
- Präsentationen, Hausaufgaben, sonstige Aufgaben etc.

4 Kategorien von der Verarbeitung betroffener Personen

- Beschäftigte des Auftraggebers, insbesondere Lehrkräfte, sowie
- sonstige berechtigte Benutzer des Auftraggebers, insbesondere Schüler und deren Eltern.

Anhang 2 zur Vereinbarung zur Auftragsverarbeitung: Technische und organisatorische Maßnahmen

I. Vertraulichkeit

1. Zutrittskontrolle

a. Die Räumlichkeiten des Auftragnehmers, in denen Kundendaten verarbeitet werden, sind gegen den Zutritt Unbefugter zu sichern. Dazu sind die Eingänge zu den Räumlichkeiten mit Sicherheits- oder Magnetkartenschlössern zu sichern. Türen, Tore und Fenster sind außerhalb der Betriebszeiten fest zu verschließen.

b. Die Vergabe von Zutrittsberechtigungen und von Schlüsseln, Magnetkarten, Ausweisen sowie anderen den Zutritt ermöglichenden Identitätsmerkmalträgern ist für die Laufzeit des Vertrags nachvollziehbar in Form einer aktuellen Auflistung der ausgegebenen Schließmittel und Zutrittsberechtigungen zu dokumentieren.

c. Sofern zur Verarbeitung von Kundendaten Server eingesetzt werden, sind diese in einem separaten Serverraum oder Rechenzentrum unterzubringen, welche durch eine Zutrittskontrollanlage gegen den Zutritt Unbefugter gesondert gesichert sind. Diese Räume sind einbruchhemmend zu schützen. Der Zutritt zu diesen Räumlichkeiten ist auf das zur Wartung und Instandsetzung erforderliche Maß sowie auf die im Übrigen konkret erforderlichen Personen zu beschränken.

2. Zugangskontrolle

a. Die zur Verarbeitung von Kundendaten eingesetzten informationsverarbeitenden Systeme des Auftragnehmers sind durch Authentifikationssysteme zu schützen. Dabei ist der Auftragnehmer zum Einsatz von Zugangsberechtigungen verpflichtet, die mindestens Benutzerkennungen und komplexe Passwörter vorsehen.

b. Authentifikationsdaten sind geheim zu halten und gegenüber unbefugten Dritten nicht bekannt zu geben. Der Auftragnehmer ist insbesondere verpflichtet, diese Authentifikationsdaten nicht im Klartext aufzubewahren. Jede Vergabe von Authentifikationsdaten ist für die Laufzeit des Vertrags zu dokumentieren.

c. Authentifikationsdaten werden ausschließlich persönlich verwendet. Jegliche Weitergabe hat zu unterbleiben. Sofern Unbefugte Kenntnis von Zugangsdaten erhalten, zeigt der Auftragnehmer dies dem Auftraggeber unverzüglich an.

d. Die Wahl von Passwörtern erfolgt in ausreichender Komplexität und Güte. Ausreichende Komplexität und Güte bedeutet mindestens eine Länge von acht Zeichen bei Nutzung von drei der folgenden vier Kategorien: Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.

e. Soweit auf informationsverarbeitenden Systemen des Auftragnehmers das Betriebssystem oder die eingesetzte Software die Möglichkeit bieten, Formulareingaben und/oder Passwörter zu speichern, ist der Auftragnehmer verpflichtet, diese Funktionalität zu deaktivieren.

f. Die Vergabe von Fernwartungszugängen, welche den Zugriff auf Kundendaten ermöglichen, ist dem Auftragnehmer nur nach Freigabe durch den Auftraggeber gestattet.

3. Zugriffskontrolle

a. Sofern Kundendaten auf informationsverarbeitenden Systemen des Auftragnehmers gespeichert werden, ist für sämtliche Zugriffe auf Kundendaten ein abgestuftes und geeignet granulares Rechtesystem einzurichten und technisch zu implementieren. Dadurch ist sicherzustellen, dass die Zugriffsrechte so ausgestaltet sind, dass sie nur den für die Leistungserbringung eingesetzten beschäftigten Personen jeweils zur Erfüllung der konkreten Aufgaben den Zugriff auf Kundendaten im notwendigen Umfang erlauben. Dabei ist die Vergabe von Administratorenrechten auf das zwingend erforderliche Maß an beschäftigten Personen des Auftragnehmers zu begrenzen. Die Rechtevergabe ist für die Laufzeit des Vertrags zu dokumentieren.

b. Sofern der Auftragsnehmer zur Leistungserbringung nach dem Vertrag Abbilder (Scans) von Originaldokumenten mit Kundendaten in elektronischer Form verarbeitet, sind die resultierenden Bilddateien gegen Zugriff von Unbefugten zu schützen.

c. Bei den zur Verarbeitung von Kundendaten eingesetzten informationsverarbeitenden Systemen des Auftragnehmers sind Bildschirme oder andere Ausgabegeräte so anzuordnen, dass unbeteiligte Hilfspersonen und sonstige Dritte keinen Einblick in Kundendaten nehmen können.

d. Soweit die Verarbeitung von Kundendaten in Form einer nicht automatisierten Datei (z.B. in einer strukturierten Akte oder Ablage) erfolgt, sind die Maßgaben dieser Ziffer zur Zugriffskontrolle sinngemäß anzuwenden.

4. Trennungskontrolle

Der Auftragnehmer ist verpflichtet, Kundendaten so zu verarbeiten, dass eine Trennung der Kundendaten von Daten anderer Auftraggeber oder Eigendaten des Auftragnehmers gewährleistet ist. Insbesondere ist sicherzustellen, dass Kundendaten jederzeit identifiziert und auch vollständig gelöscht werden können.

5. Pseudonymisierung

a. Der Auftragnehmer ist verpflichtet, Kundendaten vornehmlich pseudonymisiert zu verarbeiten, sofern die Leistungserbringung dadurch weiterhin möglich bleibt und nicht beeinträchtigt wird. Dieser Aufwand muss in einem angemessenen Verhältnis zum angestrebten Schutzziel stehen.

b. Pseudonyme sind derart zu erzeugen, dass personenbezogene Daten durch eindeutige künstliche Indizes, Scrambles oder zufällige Zeichenketten ersetzt werden.

c. Die Informationen zur Auflösung von Pseudonymen sind zu verschlüsseln und der Zugriff nur Berechtigten des Auftragnehmers zu gewähren.

II. Integrität

1. Weitergabekontrolle

a. Der Auftragnehmer hat sicherzustellen, dass Kundendaten nicht unbefugt kopiert (insbesondere auf externe Datenträger gespeichert), weitergegeben und/oder gelöscht werden können.

b. Sofern der Auftragnehmer informationsverarbeitende Systeme mit nicht-flüchtigem Speicher (beispielsweise Netzwerkdrucker oder Scanner) einsetzt, ist durch den Auftragnehmer sicherzustellen, dass durch diese Systeme keine Kundendaten über den unmittelbar zur Vertragsdurchführung erforderlichen Umfang hinaus gespeichert werden. Der Auftragnehmer hat durch technische Maßnahmen sicherzustellen, dass Dritte (insbesondere ggf. zur Wartung der Systeme eingesetzte externe Dienstleister) nicht auf Kundendaten zugreifen können.

2. Eingabekontrolle

Sofern der Auftragnehmer Kundendaten verarbeitet, so hat er bis zur Löschung der Kundendaten durch Protokollierung oder organisatorische Maßnahmen sicherzustellen, dass auf Verlangen des Auftraggebers jederzeit, auch nachträglich, zuverlässig festgestellt werden kann, wann und von wem welche Kundendaten verarbeitet wurden (mindestens durch eine Protokollierung der Benutzerkennung der Daten verarbeitenden Person, des geänderten Datums und des Zeitpunktes der Änderung).

3. Löschen

a. Der Auftragnehmer hat sämtliche löschbaren elektronischen Datenträger (insbesondere Festplatten, USB-Sticks, Disketten, Bänder), die Kundendaten enthalten, nicht wieder herstellbar zu löschen.

b. Der Auftragnehmer hat sämtliche Papierdokumente und alle nicht-löschbaren Datenträger (einschließlich sämtlicher Fehldrucke bzw. Fehlspeicherungen, sowie CDs und DVDs), die Kundendaten enthalten, mit einem handelsüblichen Dokumentenvernichter gemäß der

Sicherheitsstufe 3 gemäß DIN-Norm 32757 oder einem mindestens gleichwertigen Verfahren zu vernichten. Defekte magnetische Datenträger, die nicht wie oben angegeben mechanisch vernichtet werden können (z.B. defekte Festplatten), sind mittels eines zugelassenen Löschgerätes nach DIN 33858 zu löschen.

III. Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

a. Der Auftragnehmer hat Kundendaten durch technische und organisatorische Maßnahmen vor Verlust durch zufällige, fahrlässige oder vorsätzliche Löschung oder Veränderung zu schützen.

b. Sicherungskopien von beim Auftragnehmer auf informationsverarbeitenden Systemen gespeicherten Kundendaten sind nach denselben Maßgaben wie Originaldaten zu behandeln, insbesondere sind sie gegen unbefugten Zugriff zu sichern.

2. Widerstandsfähigkeit

a. Auf den vom Auftragnehmer verwendeten Clients sind, soweit technisch möglich, gegen Manipulation gesicherte Schutzsoftware/Virenscanner mit regelmäßigen Updates, sowie eine Firewall zu betreiben.

b. Sämtliche vom Auftragnehmer verwendete Software ist aktualisiert zu halten und sicherheitsrelevante Aktualisierungen (insbesondere Updates, Patches, Fixes) sind einzuspielen, nachdem diese vom Hersteller der Software allgemein verfügbar gemacht wurden.

c. Von Dritten stammende Dateien, insbesondere mit ausführbaren Inhalten, dürfen nur nach vorheriger manueller und/oder automatischer Prüfung ihres Inhalts auf schädliche Inhalte auf die informationsverarbeitenden Systeme des Auftragnehmers übertragen werden.

3. Verschlüsselung

Besteht eine vertraglich vereinbarte Pflicht zur Verschlüsselung von Kundendaten, wendet der Auftragnehmer, vorbehaltlich der vorherigen anderweitigen Absprache mit dem Auftraggeber, ein Verfahren an, welches in der „Technischen Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der jeweils aktuell gültigen Fassung empfohlen wird, und hält dabei zumindest folgende Standards ein:

- Symmetrische Blockchiffren AES mit einer Schlüssellänge von mindestens 128 Bit;
- Asymmetrische Chiffren das Verfahren RSA mit einer Schlüssellänge von mindestens 2048 Bit;
- Für Hash-Verfahren SHA-256 oder höher.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Auftragskontrolle

a. Die beim Auftragnehmer zur Durchführung beschäftigten Personen werden vor dem Einsatz über die allgemeinen Grundsätze der Verarbeitung von Kundendaten sowie über die sich aus dem Vertrag ergebenden spezifischen Anforderungen des Datenschutzes und der Datensicherheit der Verarbeitung von Kundendaten geschult.

b. Die beim Auftragnehmer beschäftigten Personen werden auf die Vertraulichkeit und den Schutz personenbezogener Daten schriftlich verpflichtet.

c. Die Durchführung von Schulungen und die Einhaltung der Verpflichtungen werden vom Auftragnehmer während der Laufzeit des Vertrages dokumentiert und vorgehalten.

d. Der Auftragnehmer stellt sicher, dass die vertraglich vereinbarten Regelungen zur Verarbeitung von Kundendaten eingehalten und umgesetzt werden.

2. Datenschutz-Management

Der Auftragnehmer hat entsprechende Regelungen und Maßnahmen in allen informationsverarbeitenden Systemen und Prozessen gesetzeskonform umzusetzen. Hierzu gehört im Rahmen des zu implementierenden Managementsystems beim Auftragnehmer insbesondere:

- Jährliche Datenschutzschulung der beschäftigten Personen samt der Verpflichtung auf das Datengeheimnis;
- Kontrolle der informationsverarbeitenden Systeme, Prozesse und eingesetzten Dienstleister;
- Etablierung einer angemessenen Datenschutzorganisation;
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

3. Vorfalls-Management

a. Der Auftragnehmer unterhält einen entsprechenden Meldeprozess für alle im Rahmen der Verarbeitung von Kundendaten eingesetzten informationsverarbeitenden Systeme und Prozesse zur Meldung von Sicherheitsvorfällen und unterrichtet alle zur Auftragserfüllung eingesetzten Personen über diesen Prozess.

b. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über identifizierte Sicherheitsvorfälle.

c. Der Auftragnehmer dokumentiert alle Sicherheitsvorfälle und die nachgelagert veranlassten Maßnahmen für die Dauer der Leistungserbringung.

Anlage 3 zur Vereinbarung zur Auftragsverarbeitung: Beauftragte Unterauftragnehmer

Firma	**Anschrift**	**Art der Zusammenarbeit**
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855, Luxemburg	Hosting der Online-Lernplattform „eStudy.fm“