Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen dem

für die Datenverarbeitung verantwortlichem Unternehmen

(Verantwortlicher)

- nachstehend „Auftraggeber“ genannt

und der

Tutoolio GmbH

Bonngasse 10, 53111 Bonn

vertreten durch den Geschäftsführer Herrn Stefan Deges

- Auftragsverarbeiter - nachstehend „Auftragnehmer“ genannt.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Auftragnehmer stellt dem Auftraggeber Produkte, Anwendungen und Dienste als Software-as-Service (SaaS) zur Verfügung.

Die Produkte, Anwendungen und Dienste umfassen Funktionen zur Verwaltung, Organisation und Durchführung von E-Learning-Kursen (unterstützt durch technische Standards wie z. B. AICC, SCORM, xAPI, cmi5 und LTI), Online-Veranstaltungen (wie z. B. Webinare), Präsenz-Veranstaltungen (wie z. B. Seminare und Workshops) und Phishing-Simulationen sowie zum Tracking, zur Dokumentation und zur Analyse von Lernfortschritten, Teilnehmeraktivitäten und Leistungsbewertungen.

Die Bereitstellung und Nutzung erfolgen als Software-as-a-Service (SaaS). Das bedeutet, dass die Produkte, Anwendungen und Dienste und die dazugehörige IT-Infrastruktur durch den Auftragnehmer entwickelt und betrieben und vom Auftraggeber als Dienstleistung genutzt werden. Die Bereitstellung und Nutzung erfolgen über das Internet bzw. durch technische Schnittstellen und Protokolle, etwa mittels eines Webbrowsers (Cloud-Computing).

Dieser Vertrag regelt die Verarbeitung von personenbezogenen Daten durch den Auftragnehmer bei der Nutzung der Softwares durch den Auftraggeber bzw. durch ihn bestimmte natürliche Personen.

(2) Dauer

Die Dauer (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

2. Konkretisierung des Auftragsinhalts

(1) Zwecke und Arten der Verarbeitung von Daten

Zum Zwecke der Verwaltung, Organisation und Durchführung von E-Learning-Kursen, Online-Veranstaltungen, Präsenz-Veranstaltungen und Phishing-Simulationen sowie zum Tracking, zur Dokumentation und zur Analyse von Lernfortschritten, Teilnehmeraktivitäten und Leistungsbewertungen werden personenbezogene Daten erfasst, erhoben, organisiert, geordnet, gespeichert, ausgelesen, abgefragt, verwendet, durch Übermittlung offengelegt, abgeglichen, verknüpft, angepasst, verändert, eingeschränkt und gelöscht.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(2) Betroffene Personen

Betroffene Personen im Sinne von Art. 4 Nr. 1 DSGVO sind durch den Auftraggeber bestimmte Personen, deren personenbezogene Daten im Rahmen der Nutzung der Produkte, Anwendungen und Dienste verarbeitet werden.

(3) Art der personenbezogenen Daten

Gegenstand der Verarbeitung personenbezogener Daten sind die folgenden Datenarten/-kategorien:

- Account-/Logindaten
- Personen-/Personaldaten
- Kontakt-/Kommunikationsdaten
- Leistungs-/Qualifikationsdaten
- Online-/Nutzungsdaten

3. 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.

4. Sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 37 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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. Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

b) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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. Eine gesetzliche Verpflichtung kann sich jedoch

nur aus dem Recht der EU oder des EU-Mitgliedstaats, dem der Auftragnehmer unterliegt, ergeben. Der Auftragnehmer teilt dem Auftraggeber eine solche gesetzliche Verpflichtung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f) 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.

g) 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.

h) 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.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

5. Leistungsort

(1) Die Verarbeitung und Nutzung der Daten finden ausschließlich im Gebiet der Bundesrepublik Deutschland, oder in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer.

(2) Jede Verlagerung des Ortes der Leistungseinbringung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 50 DSGVO erfüllt sind.

6. Unterauftragsverhältnisse

(1) Zurzeit sind für den Auftragnehmer die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer mit der Verarbeitung von personenbezogenen Daten beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(2) Der Auftragnehmer informiert den Auftraggeber in einer angemessenen Zeit vorab 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. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

(3) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

(4) Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Personal-, Post- und Versanddienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

(5) Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Unterauftragsverarbeiter im Wege eines Vertrags, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats im Wesentlichen dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Sofern ein Unterauftragsverarbeiter seine hieraus resultierenden Pflichten verletzt, informiert der Auftragsverarbeiter den Verantwortlichen entsprechend. Der Auftragsverarbeiter stellt sicher, dass jeder Unterauftragsverarbeiter die Verpflichtungen des Auftragsverarbeiters aus diesem Vertrag sowie der DSGVO erfüllt. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Unterauftragsverarbeiters.

7. Verantwortlichkeit und Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ i.S.v. Art. 4 Nr. 7 DSGVO).

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihr Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder § 22 TDDDG besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(5) Die Produkte, Anwendungen und Dienste des Auftragnehmers sind nicht explizit für die Verarbeitung von personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO ausgelegt. Der Auftraggeber stellt sicher, dass keine besonderen Kategorien personenbezogener Daten gemäß Art. 9 Absatz 1 DSGVO in die Produkte, Anwendungen und Dienste eingegeben und beim Auftragnehmer verarbeitet werden.

8. 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 dieses Vertrags 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 DSGVO 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 Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen 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.

10. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen sind in Textform zu erteilen.

(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.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die in Folge ergänzender Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

11. 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. Gemäß Art. 28 Abs. 3 lit. g DSGVO kann sich eine solche gesetzliche Pflicht jedoch nur aus dem Recht der EU oder eines EU-Mitgliedstaats ergeben.

(2) Nach dem Ende der Laufzeit des Hauptvertrags oder früher nach Aufforderung durch den Auftraggeber 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.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Schlussbestimmungen

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(2) Änderungen und Ergänzungen dieses Vertrages und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Es gilt deutsches Recht. Der Gerichtsstand liegt in Bonn.

(4) Im Übrigen gelten die Allgemeinen Geschäftsbedingungen (kurz AGB) des Auftragnehmers. Bei etwaigen Widersprüchen zwischen diesem Vertrag und etwaigen anderen Verträgen zwischen den Parteien gehen die Regelungen dieses Vertrags vor.

(5) Sollten einzelne Bestimmungen des Vertrages gegen bestehendes Recht verstoßen oder anderweitig unwirksam sein bzw. werden oder eine ausfüllungsbedürftige Lücke aufweisen, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Vertragsparteien verpflichten sich, anstelle einer unwirksamen Bestimmung eine gültige Vereinbarung zu treffen, deren wirtschaftliche Absicht dem der unwirksamen so weit wie möglich nahekommt.

Tutoolio GmbH, Bonn im Oktober 2024

Anlage 1 - Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1. Zutrittskontrolle

Der unbefugte Zutritt zu Datenverarbeitungsanlagen wird verhindert durch:

- Schlüsselmanagement / Protokollierte Schlüsselausgabe
- Manuelle/mechanische Schließsysteme
- Besucherbuch
- Begleitung von Besuchern durch eigene Mitarbeiter

1.2. Zugangskontrolle

Die unbefugte Systembenutzung wird verhindert durch:

- Authentifizierung mit Benutzername/Passwort
- Sichere Passwörter mit Mindestvorgaben zur Passwortkomplexität
- Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls

1.3. Zugriffskontrolle

Das unbefugte Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems wird verhindert durch:

- Bedarfsgerechte Zugriffsrechte (Berechtigungskonzept)

1.4. Trennungskontrolle

Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, wird gewährleistet durch:

- Trennung von Produktiv- und Testumgebung
- Mandantenfähigkeit
- Bedarfsgerechte Zugriffsrechte (Berechtigungskonzept)

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Das unbefugte Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport wird verhindert durch:

- Einsatz von VPN
- Verschlüsselung bei der Datenspeicherung
- Verschlüsselung bei der elektronischen Übertragung
- Passwortschutz von mobilen Datenträgern

2.2. Eingabekontrolle

Ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, kann nachvollzogen werden durch:

- Benutzerbezogene Protokollierung von Eingaben, Veränderungen und Löschungen von Daten

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Der Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust wird sichergestellt durch:

- Regelmäßige Datensicherungen
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls

4. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Die rasche Wiederherstellbarkeit wird sichergestellt durch:

- Regelmäßige Datensicherungen
- Meldewege

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO):

- Datenschutzmanagement
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle

Anlage 2 - Unterauftragnehmer

1. Unterauftragnehmer:

Amazon Web Services EMEA Sàrl ("AWS Europe"), Luxembourg,

Tochtergesellschaft von

Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 89109-5210, USA

Auftragsinhalt:

Bereitstellung von AWS-Services: Amazon CloudFront, Amazon Simple Storage Service (Amazon S3), AWS CodeBuild, AWS CodeCommit, AWS CodeDeploy, AWS CodePipeline, Amazon Elastic Container Registry (Amazon ECR), Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch, Amazon Relation Database Service (Amazon RDS), Amazon Simple Email Service (Amazon SES), AWS Fargate, Amazon Elastic Computing (EC2)

Datenschutzniveau:

Ort der Leistung:

Die Bereitstellung und Nutzung der AWS-Services (die Verarbeitung aller Daten) erfolgt ausschließlich am Serverstandort Deutschland (AWS Region eu-central-1).

Es werden keine Daten an andere Serverstandorte (AWS-Regionen) übermittelt, weder an Serverstandorte (AWS-Regionen) innerhalb der EU bzw. des Europäischen Wirtschaftsraumes (EWR) noch an Serverstandorte (AWS-Regionen) in Ländern außerhalb der EU / des EWR (sichere oder unsichere Drittländer).

Technische Maßnahmen:

Die Übermittlung von Daten an andere Serverstandorte (AWS-Regionen) wird durch dokumentierte Verschlüsselungs-, Lösch- und Überwachungsfunktionen verhindert.

Die Dokumentationen sind verfügbar unter:

https://aws.amazon.com/de/compliance/privacy-features/

Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO:

Amazon Web Services ist zertifiziert nach dem EU-U.S. Data Privacy Framework (Nachfolger des „Privacy Shields“). Die Zertifizierung umfasst Non-HR-Daten.

Das U.S. Department of Commerce veröffentlicht eine Liste, anhand welcher die Zertifizierung überprüft werden kann:

https://www.dataprivacyframework.gov/list

Die Zertifizierung umfasst keine HR-Daten („Human Resources Data“; Beschäftigtendaten / Daten im Beschäftigungskontext). Diese sind legitimiert durch:

Geeignete Garantien nach Art. 46 Abs. 2 lit. c DSGVO:

In dem Vertrag über die Auftragsverarbeitung (Data Processing Agreement, kurz: DPA) gemäß Art. 28 Abs. 3 DSGVO werden die Standardvertragsklauseln gem. Durchführungsbeschluss (EU) 2021/914 der EU-Kommission v. 04.06.2021 – Az. C(2021) 3972, ABl. EU Nr. L 199/31 vom 07.06.2021 angewendet.

Zertifizierungen des Unterauftragnehmers:

- ISO 27001 (Informationssicherheit)
- ISO 27017 (Cloud-Sicherheit)
- ISO 27018 (Cloud-Datenschutz)
- BSI Cloud Computing Compliance Criteria Catalogue (kurz: BSI C5) des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Weitere Informationen:

https://aws.amazon.com/de/compliance/germany-data-protection/

https://aws.amazon.com/de/compliance/gdpr-center/

2. Unterauftragnehmer:

Rustici Software LLC, 210 Gothic Ct #100, Franklin, TN 37067, USA

Auftragsinhalt:

Bereitstellung von Software-Komponenten zum Importieren und Abspielen von digitalen Lernmedien in den Standards LTI, AICC, cmi5, SCORM und Tin Can API/xAPI sowie zum Tracken von Lernaktivitäten.

Datenschutzniveau:

Ort der Leistung:

Die Bereitstellung und Nutzung der Software-Komponenten von Rustici Software LLC erfolgt über Amazon Web Services (siehe Unterauftragnehmer Nr. 1, Seite 11). Die Bereitstellung und Nutzung der Software-Komponenten erfolgt ebenfalls ausschließlich am Serverstandort Deutschland (AWS Region eu-central-1).

Es werden keine Daten an andere Serverstandorte (AWS-Regionen) übermittelt, weder an Serverstandorte (AWS-Regionen) innerhalb der EU bzw. des Europäischen Wirtschaftsraumes (EWR) noch an Serverstandorte (AWS-Regionen) in Ländern außerhalb der EU / des EWR (sichere oder unsichere Drittländer).

Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO:

Rustici Software LLC ist zertifiziert nach dem EU-U.S. Data Privacy Framework (Nachfolger des „Privacy Shields“). Die Zertifizierung umfasst Non-HR-Daten und HR-Daten („Human Resources Data“; Beschäftigtendaten / Daten im Beschäftigungskontext).

Das U.S. Department of Commerce veröffentlicht eine Liste, anhand welcher die Zertifizierung überprüft werden kann:

https://www.dataprivacyframework.gov/list

Geeignete Garantien nach Art. 46 Abs. 2 lit. c DSGVO:

In dem Vertrag über die Auftragsverarbeitung (Data Processing Agreement, kurz: DPA) gemäß Art. 28 Abs. 3 DSGVO werden die Standardvertragsklauseln gem. Durchführungsbeschluss (EU) 2021/914 der EU-Kommission v. 04.06.2021 – Az. C(2021) 3972, ABl. EU Nr. L 199/31 vom 07.06.2021 angewendet.

Zertifizierungen des Unterauftragnehmers:

- ISO 27001 (Informationssicherheit)

Weitere Informationen:

https://ltgplc.com/privacy-notice/

https://security.rusticisoftware.com/?_ga=2.257275976.277215554.1619594162-88742652.1619594162

https://rusticisoftware.com/security-certifications/

3. Unterauftragnehmer:

Lotus Awareness UG (haftungsbeschränkt), Brunnenstraße 14, 56075 Koblenz

Auftragsinhalt:

Bereitstellung von Software zur Verwaltung, Organisation und Durchführung von Phishing-Simulationen sowie zum Tracking, zur Dokumentation und zur Analyse von Teilnehmeraktivitäten.

Datenschutzniveau:

Ort der Leistung:

Die Bereitstellung und Nutzung der Software der Lotus Awareness UG (haftungsbeschränkt) erfolgt über Amazon Web Services (siehe Unterauftragnehmer Nr. 1, Seite 11). Die Bereitstellung und Nutzung der Software-Komponenten erfolgt ebenfalls ausschließlich am Serverstandort Deutschland (AWS Region eu-central-1).

Es werden keine Daten an andere Serverstandorte (AWS-Regionen) übermittelt, weder an Serverstandorte (AWS-Regionen) innerhalb der EU bzw. des Europäischen Wirtschaftsraumes (EWR) noch an Serverstandorte (AWS-Regionen) in Ländern außerhalb der EU / des EWR (sichere oder unsichere Drittländer).

Falls der integrierte Mailservice genutzt wird (optional): Der Mail-Versand erfolgt ausschließlich über Server in den EU-Standorten Deutschland und Belgien, die sich im Geltungsbereich der DSGVO befinden (weitere Informationen dazu stellt der Unterauftragnehmer bereit, s. unten).

Auftragsverarbeitungsvertrag (AV-Vertrag) gemäß Artikel 28 DSGVO:

Im Rahmen der Zusammenarbeit mit Lotus Awareness UG (haftungsbeschränkt) wurde ein Auftragsverarbeitungsvertrag (AV-Vertrag) gemäß Artikel 28 DSGVO geschlossen. Dieser Vertrag regelt die Pflichten und Verantwortlichkeiten des Unterauftragnehmers im Hinblick auf die Verarbeitung personenbezogener Daten, wie in den Artikeln 28 bis 32 DSGVO festgelegt. Der Unterauftragnehmer ist verpflichtet, alle datenschutzrechtlichen Anforderungen der DSGVO einzuhalten und angemessene technische sowie organisatorische Maßnahmen zum Schutz der Daten gemäß Artikel 32 DSGVO zu ergreifen.

Regelmäßige Audits des Unterauftragnehmers:

Der Unterauftragnehmer wird in regelmäßigen Abständen auditiert, um die Einhaltung der im Auftragsverarbeitungsvertrag festgelegten datenschutzrechtlichen Verpflichtungen und der technischen sowie organisatorischen Maßnahmen gemäß Artikel 32 DSGVO sicherzustellen. Diese Audits dienen der kontinuierlichen Überwachung und Verbesserung der Datensicherheitsmaßnahmen. Auf Grundlage von Artikel 28 Abs. 3 lit. h DSGVO ist der Unterauftragnehmer verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen und Audits oder Inspektionen zu ermöglichen, um die Einhaltung der datenschutzrechtlichen Anforderungen nachzuweisen. Zudem erfolgt die Überprüfung der Maßnahmen gemäß Artikel 24 Abs. 1 DSGVO, um die fortlaufende Einhaltung sicherzustellen.

Weitere Informationen:

https://lotus-awareness.com/av-vertrag-v1-2024-09-23/

https://lotus-awareness.com/datenschutz/