Auftragsverarbeitung gemäß Art. 28 DSGVO (AVV reteach)

Stand: 08.2026

Zwischen dem reteach Kunden (Verantwortlicher und Auftraggeber nach diesem Vertrag) und der Susell GmbH (Joachimstrasse 7, 10119 Berlin) als Anbieter der reteach Produkte und Auftragnehmer nach diesem Vertrag wird folgender Vertrag geschlossen.

Vorbemerkung

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Vertrag über die Nutzung des reteach Produktes des Auftragsverarbeiters durch den Verantwortlichen. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Umsetzung eigener Geschäftszwecke im Zusammenhang mit diesem Vertrag. Eine Übertragung von Funktionen ist ausdrücklich nicht beabsichtigt.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 DSGVO. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.

(2) Sofern in diesem Vertrag der Begriff »Datenverarbeitung« oder »Verarbeitung« benutzt wird, gilt die Definition des Art. 4 Nr. 2 DSGVO.

(3) Dieser Vertrag ergänzt die Allgemeinen Geschäftsbedingungen des Auftragnehmers (die „AGB“). Für datenschutzrechtliche Fragen geht er den AGB vor. Die Haftung des Auftragnehmers richtet sich abschließend nach § 8 der AGB; dieser Vertrag begründet keine darüber hinausgehende Haftung (vgl. § 2 Abs. 5 AGB).

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

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

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen erfolgen in Textform (z. B. E-Mail).

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

(5) Besteht eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder eine sonstige für den Auftraggeber geltende Meldepflicht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und der Weisungen des Auftraggebers. Ausgenommen sind gesetzliche Verarbeitungspflichten; in diesem Fall teilt der Auftragnehmer dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Verarbeitung findet grundsätzlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des EWR statt. Die in Anlage 2 Abschnitt A genannten Unterauftragnehmer verarbeiten ausschließlich in der EU; ein Drittlandtransfer findet im Regelbetrieb der Plattform nicht statt. Soweit der Auftraggeber einzelne Module oder Funktionen nutzt, für die in Anlage 2 Abschnitt B zusätzliche Unterauftragnehmer ausgewiesen sind, kann eine Verarbeitung auch in Drittländern stattfinden. Soweit eine Übermittlung in ein Drittland erfolgt oder ein Zugriff aus einem Drittland nicht ausgeschlossen werden kann, stützt der Auftragnehmer die Übermittlung auf einen Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO, soweit ein solcher für den jeweiligen Empfänger gilt, und im Übrigen auf die Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO nebst erforderlicher Zusatzmaßnahmen. Entfällt ein Angemessenheitsbeschluss, auf den sich eine Übermittlung stützt, gelten für diese Übermittlung ohne weiteres die Standardvertragsklauseln; der Auftragnehmer unterrichtet den Auftraggeber unverzüglich und ergreift die erforderlichen Maßnahmen. Anlage 2 weist die für den jeweiligen Unterauftragnehmer maßgebliche Transfergrundlage aus.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die im Auftrag verarbeiteten Daten im erforderlichen Maß gesichert und vor unbefugter Kenntnisnahme Dritter geschützt sind. Änderungen in

der Organisation der Datenverarbeitung, die für die Sicherheit der Daten erheblich sind, stimmt er vorab mit dem Auftraggeber ab.

(5) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn eine Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt, und ist berechtigt, deren Durchführung bis zur Bestätigung oder Änderung auszusetzen. Kann der Auftragnehmer darlegen, dass eine Verarbeitung nach Weisung zu einer Haftung nach Art. 82 DSGVO führen kann, steht ihm frei, die weitere Verarbeitung bis zur Klärung auszusetzen.

(6) Der Auftragnehmer verarbeitet die Daten des Auftraggebers getrennt von anderen Daten. Eine physische Trennung ist nicht zwingend erforderlich.

(7) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen berechtigt sind.

(8) Der Auftraggeber gestattet dem Auftragnehmer, personenbezogene Daten zu anonymisieren und die so entstandenen aggregierten und anonymisierten Daten für Zwecke der Statistik, des Benchmarking, der Fehleranalyse sowie der Produktentwicklung und -verbesserung zu nutzen. Der Klarstellung halber halten die Parteien fest, dass hierbei weder personenbezogene Daten noch vertrauliche Informationen des Auftraggebers offengelegt oder Dritten gegenüber sichtbar werden.

5. Datenschutzbeauftragter des Auftragnehmers

Der Auftragnehmer benennt einen Datenschutzbeauftragten nach Art. 37 DSGVO, sofern dieser zu benennen ist, und trägt Sorge für dessen Qualifikation und Fachwissen. Name und Kontaktdaten teilt er dem Auftraggeber auf Anforderung mit. Anfragen zum Datenschutz sind an datenschutz@reteach.com zu richten.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer teilt dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften, gegen die getroffenen vertraglichen Vereinbarungen oder gegen erteilte Weisungen unverzüglich mit. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch die Verarbeitung für den Auftraggeber betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer unterstützt den Auftraggeber bei der Umsetzung dieser Meldepflichten. Er teilt dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten unverzüglich, spätestens aber binnen 48 Stunden ab eigener Kenntnis mit. Beruht der Vorfall auf einem Ereignis im Verantwortungsbereich eines Unterauftragnehmers, bemisst sich diese Frist ab dem Zeitpunkt, zu dem der Auftragnehmer hiervon Kenntnis erlangt.

Die Meldung des Auftragnehmers enthält insbesondere:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der betroffenen Kategorien und der ungefähren Zahl der betroffenen Datensätze;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12–23 DSGVO. Es gelten ergänzend die Regelungen der Ziff. 11.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei der Einhaltung der Pflichten nach Art. 32–36 DSGVO.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der datenschutzrechtlichen Vorschriften, der vertraglichen Regelungen und der erteilten Weisungen durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren. Die Kontrolle erfolgt gestuft: zunächst durch Vorlage von Dokumentationen, Zertifikaten und Nachweisen, sodann durch Fernprüfung (z. B. Fragebogen oder Videokonferenz). Eine Prüfung vor Ort kommt nur in Betracht, wenn die vorstehenden Stufen zur Klärung nicht ausreichen; sie ist auf die Geschäftsräume des Auftragnehmers beschränkt und mit angemessener Vorankündigung während der üblichen Geschäftszeiten durchzuführen. Rechenzentren der Unterauftragnehmer sind hiervon ausgenommen; insoweit legt der Auftragnehmer die vorhandenen Nachweise und Zertifikate seiner Unterauftragnehmer vor.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle nach Absatz 1 erforderlich ist.

(3) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO die erforderlichen Auskünfte zu erteilen und der zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist zulässig. Die bei Vertragsschluss bestehenden Unterauftragsverhältnisse sind in Anlage 2 angegeben; der Auftraggeber stimmt deren Einsatz zu. Der Auftragnehmer informiert den Auftraggeber über die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer mit einer Frist von vier (4) Wochen vor Wirksamwerden. Der Auftraggeber kann innerhalb dieser Frist aus einem wichtigen datenschutzrechtlichen Grund in Textform Einspruch erheben. Erhebt er Einspruch, suchen die Parteien eine einvernehmliche Lösung; kommt eine solche nicht zustande, ist jede Partei berechtigt, den Vertrag mit Wirkung zum Ende des laufenden Kalendermonats zu kündigen.

(2) Ändert sich die Liste der Unterauftragnehmer nach dem Verfahren des Absatzes 1, wird die geänderte Anlage 2 mit Ablauf der dort genannten Frist Bestandteil dieses Vertrages, ohne dass es einer erneuten Vereinbarung bedarf. Die jeweils aktuelle Fassung der Anlage 2 ist unter https://www.reteach.com/agb/ abrufbar. Erhebt der Auftraggeber fristgerecht Einspruch, gilt Absatz 1 Satz 3.

(3) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Er kontrolliert insbesondere vorab und regelmäßig während der Vertragsdauer, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen getroffen hat.

(4) Der Auftragnehmer stellt sicher, dass die in diesem Vertrag vereinbarten Regelungen und ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Er schließt mit dem Unterauftragnehmer einen Vertrag, der den Voraussetzungen des Art. 28 DSGVO entspricht.

(5) Ist die Beauftragung eines Unterauftragnehmers mit einer Übermittlung in ein Drittland verbunden, gelten zusätzlich die Vorgaben aus Ziff. 4 Abs. 2.

(6) Nicht als Unterauftragsverhältnisse gelten reine Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben (z. B. Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zur Leistungserbringung, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste). Der Auftragnehmer trägt gleichwohl dafür Sorge, dass auch insoweit angemessene technische und organisatorische Maßnahmen getroffen wurden. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis dar, wenn dabei auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten verpflichtet, die er im Zusammenhang mit dem Auftrag erhält oder zur Kenntnis erlangt. Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber teilt dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mit.

(2) Der Auftragnehmer sichert zu, dass ihm die geltenden datenschutzrechtlichen Vorschriften bekannt sind, dass er seine Beschäftigten mit den maßgeblichen Bestimmungen des Datenschutzes vertraut macht und die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet und über die Weisungen des Auftraggebers informiert hat.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer unterstützt ihn bei der Bearbeitung von Anträgen nach Art. 12–23 DSGVO und trägt insbesondere dafür Sorge, dass die erforderlichen Informationen unverzüglich erteilt werden, damit der Auftraggeber seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Einschränkung oder Löschung – erforderlich ist, trifft er die erforderlichen Maßnahmen nach Weisung des Auftraggebers und unterstützt ihn nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen zu anderen Zwecken zu nutzen oder Dritten zugänglich zu machen. Die Verpflichtungen gelten für drei (3) Jahre über das Ende des Vertrages hinaus; ergänzend gilt § 9 der AGB.

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

13. Vergütung

Eine Vergütung des Auftragnehmers nach diesem Vertrag ist gesondert zu vereinbaren; hierfür genügt die Textform (z. B. E-Mail). Unterstützungsleistungen, die über die gesetzlich und vertraglich geschuldeten Mitwirkungspflichten hinausgehen, werden gesondert vergütet.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind, insbesondere nach Art. 32 DSGVO.

(2) Der bei Vertragsschluss bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 3 beigefügt. Änderungen sind zulässig, soweit das bestehende Schutzniveau nicht unterschritten wird. Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, teilt der Auftragnehmer dem Auftraggeber mit. Der Auftraggeber kann jederzeit eine aktuelle Fassung anfordern.

(3) Der Auftragnehmer kontrolliert die getroffenen Maßnahmen regelmäßig und anlassbezogen auf ihre Wirksamkeit und informiert den Auftraggeber, wenn Optimierungs- oder Änderungsbedarf besteht.

15. Dauer des Auftrags

Laufzeit und Kündigung dieses Vertrages richten sich nach den Bestimmungen des Hauptvertrages. Eine Kündigung des Hauptvertrages bewirkt automatisch auch die Kündigung dieses Vertrages. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

16. Beendigung

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, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen, soweit keine gesetzliche Aufbewahrungspflicht besteht.

17. Schlussbestimmungen

Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB wird hinsichtlich der verarbeiteten Daten ausgeschlossen. Dieser Vertrag wird elektronisch abgeschlossen. Sollten einzelne Teile dieses Vertrages unwirksam sein, berührt dies die Wirksamkeit der übrigen Regelungen nicht. Diese Vereinbarung tritt mit Zustimmung durch den Auftraggeber in Kraft und ersetzt alle zuvor geschlossenen Vereinbarungen zur Auftragsverarbeitung.

Anlage 1 – Gegenstand des Auftrags

1. Gegenstand, Art und Zweck der Verarbeitung

Der Auftragnehmer stellt für den Auftraggeber eine cloudbasierte Software zur Erstellung und Bereitstellung von Lerninhalten sowie zur Verarbeitung von Lernaktivitäten und Lernständen zur Verfügung. Die Software dient dem digitalen Training, der Schulung, Aus-, Fort- und Weiterbildung sowie der Kommunikation zwischen den Anwendern.

Ist das Modul Phishing Awareness gebucht, umfasst die Verarbeitung zusätzlich die Durchführung von Phishing-Simulationen sowie die Erfassung und Auswertung der Reaktionen der Empfänger zum Zweck der Sicherheitsschulung.

2. Art(en) der personenbezogenen Daten

- E-Mail-Adresse des Nutzers / Anmeldename
- persönliches Passwort
- Protokolldaten über die Lernaktivität des Nutzers (durchgeführte Aktivitäten, Zeitpunkt, weitere Verkehrsdaten)
- Teilnahme-, Abschluss- und Zertifikatsdaten
- Vertrags- und Zahlungsdaten
- Vom Auftraggeber optional festgelegte weitere Daten: Vorname, Nachname, Titel, Anrede, Geburtsdatum, Adresse, Stadt, Land sowie weitere Profildaten
- Bei gebuchtem Modul Phishing Awareness zusätzlich: Reaktionsdaten zu Phishing-Simulationen je Empfänger (Zustellung, Öffnen, Klick, Eingabe von Daten, Meldung durch den Nutzer) sowie technische Verbindungsdaten (IP-Adresse). Die Zuordnung zum Empfänger erfolgt über eine pseudonyme Kennung; eine Auflösung ist ausschließlich innerhalb des Systems des Auftragnehmers möglich.

3. Kategorien betroffener Personen

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers
- Teilnehmende / Lehrende / Schüler / Studierende
- Externe Trainer des Auftraggebers

4. Auswertungsmodus bei Phishing Awareness

Der Auftraggeber bestimmt als Verantwortlicher, ob die Auswertung der Kampagnenergebnisse aggregiert (Standard) oder personenbezogen erfolgt. Die personenbezogene Auswertung wird erst nach ausdrücklicher Bestätigung des Auftraggebers aktiviert, dass hierfür eine Rechtsgrundlage besteht (insbesondere § 26 BDSG bzw. Art. 6 Abs. 1 lit. f DSGVO) und eine etwaig erforderliche Beteiligung der zuständigen Arbeitnehmer- bzw. Beschäftigtenvertretung sichergestellt ist.

5. Speicherdauer und Löschung

Die Daten werden für die Dauer des Vertragsverhältnisses gespeichert und nach dessen Beendigung nach Weisung des Auftraggebers zurückgegeben oder gelöscht, soweit keine gesetzliche Aufbewahrungspflicht besteht. Für Reaktionsdaten zu Phishing-Simulationen gilt eine Speicherdauer von 24 Monaten ab Erhebung; danach werden sie gelöscht oder anonymisiert.

Anlage 2 – Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch (»Unterauftragnehmer«). Dabei handelt es sich derzeit um die nachfolgenden Unternehmen. Die Spalte „Transfergrundlage“ weist aus, worauf eine etwaige Übermittlung in ein Drittland gestützt wird (Ziff. 4 Abs. 2).

Abschnitt A – Regelbetrieb der Plattform

- Amazon Web Services Inc. (Cloud-Infrastruktur, Datenbank, Datei-Speicher und E-Mail-Versand) – Rechenzentrum: Frankfurt am Main, Region eu-central-1 (Deutschland); Unternehmenssitz: Seattle, WA (USA). Transfergrundlage: Angemessenheitsbeschluss (EU-US Data Privacy Framework), hilfsweise Standardvertragsklauseln.
- BunnyWay informacijske storitve d.o.o. (Videohosting und Auslieferung über Content Delivery Network) – Dunajska cesta 165, 1000 Ljubljana (Slowenien). Sitz in der EU, kein Drittlandtransfer. Die Anonymisierung der IP-Adressen in den Zugriffsprotokollen ist aktiviert.
- Streamdiver GmbH (Videoverarbeitung und -hosting) – Klagenfurt am Wörthersee (Österreich). Sitz in der EU, kein Drittlandtransfer.
- Datadog, Inc. (Betriebsüberwachung, Fehleranalyse und Protokollierung der Anwendung) – Verarbeitung in der Europäischen Union. Sitz der Verarbeitung in der EU, kein Drittlandtransfer. Zertifizierungen: ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2 Type II. Der Auftragnehmer filtert personenbezogene Daten, insbesondere E-Mail-Adressen, aus den übermittelten Protokolldaten heraus, soweit dies technisch möglich ist; ein vollständiger Ausschluss kann insbesondere bei Protokollen der Programmierschnittstelle nicht gewährleistet werden. Protokolldaten werden nach sieben (7) Tagen gelöscht.
- Mixpanel, Inc. (Analyse der Produktnutzung zur Fehleranalyse und Verbesserung der Anwendung) – Verarbeitung in Eemshaven (Niederlande, EU Data Residency). Sitz der Verarbeitung in der EU, kein Drittlandtransfer. Zertifizierungen: ISO 27001, ISO 27701, SOC 2 Type II. Übermittelt wird ausschließlich eine pseudonyme Nutzerkennung; Namen, E-Mail-Adressen und IP-Adressen werden nicht übertragen.

Abschnitt B – Modulgebundene Unterauftragnehmer

Die nachfolgenden Unterauftragnehmer werden nur eingesetzt, wenn der Auftraggeber das jeweils genannte Modul oder die genannte Funktion nutzt.

- Nur bei Nutzung der HRIS-Synchronisation: Kombo Technologies GmbH (Middleware für Schnittstellen zu HR-Systemen) – Kottbusser Damm 25-26, 10967 Berlin (Deutschland). Sitz in der EU, kein Drittlandtransfer.
- Nur bei Nutzung von SCORM als Kursformat:
  Rustici Software, LLC (SCORM-Verarbeitung und -hosting) – Franklin, TN (USA). Transfergrundlage: Angemessenheitsbeschluss (EU-US Data Privacy Framework), hilfsweise Standardvertragsklauseln.
- Nur bei Nutzung des eCommerce-Moduls:
  Stripe, Inc. (Zahlungsdienstleistungen) – San Francisco, CA (USA). Transfergrundlage: Angemessenheitsbeschluss (EU-US Data Privacy Framework), hilfsweise Standardvertragsklauseln.
- Nur bei gebuchtem Modul Phishing Awareness:
  Phishing Tackle Limited (technische Dienstleistungen für das Modul Phishing Awareness) – 167-169 Great Portland Street, London W1W 5PF (Vereinigtes Königreich); Verarbeitung in Rechenzentren im Vereinigten Königreich Vereinigtes Königreich (AWS London, eu-west-2). Transfergrundlage: Angemessenheitsbeschluss der Europäischen Kommission für das Vereinigte Königreich.

Der Auftragnehmer kann nach Maßgabe der Ziff. 9 weitere Unterauftragnehmer einsetzen.

Dienste, die der Auftragnehmer ausschließlich für eigene Zwecke einsetzt und bei denen er selbst Verantwortlicher ist (insbesondere Abonnementverwaltung, Rechnungsstellung, CRM sowie Vertriebs- und Marketingzwecke), verarbeiten keine personenbezogenen Daten der Nutzer des Auftraggebers und sind daher nicht Unterauftragnehmer im Sinne dieses Vertrages. Informationen hierzu enthält die Datenschutzerklärung des Auftragnehmers.

Sofern der Auftraggeber die im Kundenkonto angebotenen Integrationen zu Drittanbietern nutzt (z. B. Microsoft Teams, Zoom, Stripe oder ein HR-Management-System), stellt der Auftragnehmer lediglich eine technische Anbindung her, ohne die Drittanbieter selbst als eigene Unterauftragnehmer einzusetzen. In diesen Fällen sind die Drittanbieter Auftragsverarbeiter des Auftraggebers.

Anlage 3 – Technische und organisatorische Maßnahmen (TOM)

Art. 32 DSGVO verpflichtet zu technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. Die Maßnahmen umfassen die Pseudonymisierung, die Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, die Fähigkeit zur raschen Wiederherstellung nach einem Zwischenfall sowie ein Verfahren zur regelmäßigen Überprüfung ihrer Wirksamkeit.

Der Auftragnehmer betreibt ein Informationssicherheits-Managementsystem (ISMS), das sich an ISO 27001 orientiert und jährlich durch die Geschäftsführung überprüft und freigegeben wird. Der Auftragnehmer speichert keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in Anlage 2 gelisteten Unterauftragnehmern; ergänzend wird auf deren Maßnahmen und Zertifizierungen verwiesen.

I. Vertraulichkeit

1. Hosting und physische Sicherheit

- Die Plattform wird auf Amazon Web Services in der Region eu-central-1 (Frankfurt am Main) betrieben. Das Rechenzentrum entspricht den Standards ANSI/TIA-942-A Tier 3 oder Tier 4 und ist zertifiziert nach ISO 27001:2022, SOC 2 Type II, CSA STAR und PCI-DSS. Der Auftragnehmer verfolgt für seine eigenen Geschäftsräume einen risikobasierten Ansatz: Der physische Zugang ist auf Mitarbeitende, Auftragnehmer und autorisierte Besucher beschränkt; Besucher werden begleitet und sind zur Vertraulichkeit verpflichtet.

2. Zugangs- und Zugriffskontrolle

- Multi-Faktor-Authentifizierung ist für alle geschäftskritischen Systeme und administrativen Zugänge verpflichtend.
- Es gelten die Prinzipien Need-to-know, Least Privilege und Aufgabentrennung. Der administrative Zugang zur Infrastruktur ist auf ein minimales Team beschränkt.
- Passwort-Richtlinie: Mindestlänge 16 Zeichen, Komplexitätsanforderungen; ein zentral verwalteter Passwort-Manager ist für alle Mitarbeitenden verpflichtend.
- Zugriffsrechte werden regelmäßig überprüft; beim Ausscheiden von Mitarbeitenden werden physische und virtuelle Zugänge unverzüglich deaktiviert. Vergabe und Entzug folgen einem dokumentierten Onboarding- und Offboarding-Prozess.
- Kunden können den Zugang ihrer Nutzer über Single Sign-On (SSO/SAML) anbinden.

3. Endgerätesicherheit

- Es werden ausschließlich Firmengeräte eingesetzt; die Nutzung privater Geräte (BYOD) ist nicht gestattet. Alle Geräte werden zentral über Mobile Device Management verwaltet und verfügen über Festplattenverschlüsselung, Endpoint Protection (Antiviren-, IPS- und Firewall-Software) sowie automatisierte Sicherheitsupdates.

4. Trennungsgebot (Mandantentrennung)

- Die Mandantentrennung erfolgt mehrstufig auf Anwendungs- und Datenbankebene. Die Mandantenzugehörigkeit wird bereits bei der Authentifizierung aus dem verifizierten Token abgeleitet und auf Anwendungsebene durchgesetzt: Jede Datenbankabfrage wird automatisch um eine mandantenspezifische Filterbedingung ergänzt. Ergänzend sichern Fremdschlüssel-Constraints und mandantenbezogene Unique-Constraints auf Datenbankebene die referenzielle Integrität und verhindern Datenkollisionen zwischen Mandanten. Produktiv- und Testsysteme sind getrennt.
- Bei gebuchtem Modul Phishing Awareness wird für jeden Mandanten des Auftragnehmers eine eigene Sub-Organisation beim Unterauftragnehmer geführt; die Übertragung der Empfängerdaten erfolgt ausschließlich mandantenbezogen. Die Zuordnung von Reaktionsereignissen erfolgt über eine pseudonyme Kennung.

5. Datenklassifikation und Vertraulichkeitsverpflichtung

- Informationen werden in drei Stufen klassifiziert (Öffentlich, Intern, Vertraulich). Alle Mitarbeitenden sind vertraglich zur Vertraulichkeit verpflichtet. Der Einsatz von KI-Tools ist in einer gesonderten Richtlinie geregelt; die Eingabe von Kundendaten in öffentliche KI-Tools ist untersagt.

II. Integrität

1. Verschlüsselung

- Data at Rest: Alle Datenbanken und Dateien werden serverseitig mit AES-256 über den AWS Key Management Service (SSE-KMS) verschlüsselt. Die Schlüsselverwaltung erfolgt über AWS KMS mit kontrolliertem Zugriff durch das Infrastruktur-Team.
- Data in Transit: Sämtliche Übertragungen zwischen Client und Server sowie zwischen internen Diensten erfolgen über TLS 1.2 oder höher; HTTPS wird für die Web-Anwendung und alle API-Endpunkte erzwungen. Passwörter werden ausschließlich gehasht gespeichert.

2. Sichere Softwareentwicklung

- Alle Code-Änderungen werden vor Produktivsetzung durch mindestens zwei Engineers geprüft (Vier-Augen-Prinzip).

- Externe Penetrationstests werden jährlich durch einen spezialisierten Dienstleister durchgeführt.
- Kritische Sicherheitsupdates werden innerhalb von 24 Stunden nach Bekanntwerden eingespielt; Sicherheitsupdates werden durch das Engineering auf Dringlichkeit und Relevanz geprüft.
- Eingesetzte Abhängigkeiten und Container werden regelmäßig auf bekannte Schwachstellen geprüft; als kritisch bewertete Funde werden priorisiert behoben.

3. Eingabe-, Weitergabe- und Auftragskontrolle

- Eingabekontrolle: Protokollierung von Eingabe, Änderung und Entfernung personenbezogener Daten; individuelle Benutzernamen; Vergabe von Änderungs-, Lösch- und Bearbeitungsrechten auf Basis eines Rollenberechtigungskonzepts.
- Weitergabekontrolle: Weitergabe in anonymisierter oder pseudonymisierter Form, vereinbarte Löschfristen, Transportverschlüsselung. In den Zugriffsprotokollen des für die Videoauslieferung eingesetzten Content Delivery Network ist die Anonymisierung der IP-Adressen aktiviert. An den Dienst zur Analyse der Produktnutzung wird ausschließlich eine pseudonyme Nutzerkennung übermittelt. Aus den an den Dienst zur Betriebsüberwachung übermittelten Protokolldaten werden personenbezogene Daten, insbesondere E-Mail-Adressen, herausgefiltert, soweit dies technisch möglich ist; die Speicherdauer dieser Protokolldaten ist auf sieben Tage begrenzt.
- Auftragskontrolle: Der Auftragnehmer führt ein Verzeichnis kritischer Dienstleister und Unterauftragnehmer. Diese werden sorgfältig ausgewählt, vor Beauftragung geprüft und regelmäßig auf Einhaltung der Sicherheitsanforderungen kontrolliert.
- Secrets-Management: Zugangsdaten, API-Schlüssel und vergleichbare Geheimnisse der Infrastruktur werden zentral und zugriffsbeschränkt verwaltet. Eine Ablage im Quellcode ist ausgeschlossen. Der Zugriff ist rollenbasiert beschränkt und erfordert Multi-Faktor-Authentifizierung.

III. Verfügbarkeit und Belastbarkeit

- Recovery Point Objective (RPO): unter 10 Minuten (Point-in-Time-Recovery).
- Recovery Time Objective (RTO): unter 4 Stunden. Die Anwendungsschicht ist zustandslos (stateless) und innerhalb von Minuten neu deploybar.
- Datenbank-Backup: Point-in-Time-Recovery (minutengenau), anschließend tägliche verschlüsselte Backups für 180 Tage auf AWS S3.
- Datei-Speicher: Versionierung aller Dateien für 180 Tage, einschließlich Änderungen und Löschungen.
- Recovery-Tests: Alle 90 Tage wird die vollständige Wiederherstellung aus dem Backup in einer Testumgebung verifiziert.
- Belastbarkeit: kontinuierliche Überwachung von Infrastruktur und Anwendungen, regelmäßige Überwachung der Serverlast, Stresstests. Ein formaler Business-Continuity-Plan regelt die Wiederherstellung geschäftskritischer Systeme.

IV. Protokollierung und Reaktion auf Vorfälle

- Logs und Traces der Infrastruktur sowie der Anwendungen werden zentral erfasst und für sieben (7) Tage gespeichert.
- Der Auftragnehmer verfügt über einen formalen Incident-Response-Plan mit Severity-Klassifikation, definierten Reaktionszeiten, Eskalationswegen und Checklisten: S1 (kritisch, bestätigter Vorfall) – Erstreaktion unter 30 Minuten; S2 (Verdacht auf Kompromittierung) – unter 4 Stunden; S3 (Schwachstelle ohne Ausnutzung) – unter 24 Stunden; S4 (sicherheitsrelevante Beobachtung) – unter 72 Stunden.
- Betroffene Auftraggeber werden unverzüglich benachrichtigt, damit diese ihre Meldepflicht nach Art. 33 DSGVO erfüllen können. Die Meldung enthält Art des Vorfalls, betroffene Datenkategorien sowie ergriffene und geplante Maßnahmen.
- Schwachstellen können jederzeit an sicherheit@reteach.com gemeldet werden.

V. Löschung

- Personenbezogene Daten werden nach Beendigung des Vertragsverhältnisses oder auf Weisung des Auftraggebers gelöscht, soweit keine gesetzliche Aufbewahrungspflicht besteht.
- Reaktionsdaten aus Phishing-Simulationen werden nach 24 Monaten automatisiert gelöscht oder anonymisiert.
- Löschung und Backups: Eine Löschung erfolgt unverzüglich im Produktivsystem. Aus den Sicherungskopien werden die Daten nach Ablauf der jeweiligen Backup-Aufbewahrungsfrist entfernt; eine gezielte Löschung einzelner Datensätze aus bestehenden Sicherungskopien ist technisch nicht möglich. Die Sicherungskopien sind verschlüsselt und zugriffsbeschränkt. Sie werden zur Wiederherstellung im Störungsfall sowie in Einzelfällen zur Fehleranalyse verwendet. Werden im Rahmen einer Wiederherstellung zwischenzeitlich gelöschte Daten wiederhergestellt, werden diese nach Abschluss der Wiederherstellung erneut gelöscht, soweit die Löschanweisung dokumentiert ist.

VI. Organisation und regelmäßige Überprüfung

- Alle Mitarbeitenden absolvieren bei Einstellung und anschließend jährlich eine Schulung zur Informationssicherheit; ergänzend werden laufend Phishing-Simulationen durchgeführt.
- Verbindliche Richtlinien bestehen für Remote-Arbeit, Endgerätesicherheit, Passwort-Management und den Einsatz von KI-Tools.
- Die Einhaltung der Sicherheitsvorgaben wird regelmäßig in internen Audits überprüft; Gegenstand sind insbesondere Zugriffskontrolle, Rollentrennung und Wiederherstellungsmaßnahmen.
- Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO. Ein Datenschutzbeauftragter ist nach § 38 BDSG nicht zu bestellen; der Datenschutz wird von der Geschäftsführung verantwortet. Anfragen: datenschutz@reteach.com.
- Das Risikomanagement liegt beim jeweiligen Prozesseigentümer und ist im Risikomanagement-Handbuch beschrieben. Die ISM-Policy wird jährlich überprüft; außerordentliche Reviews erfolgen bei wesentlichen Änderungen der Bedrohungslage, der Organisationsstruktur oder der regulatorischen Anforderungen.