

# Datenschutz bei reteach

Häufige Fragen · Stand: August 2026

Diese Übersicht beantwortet die Fragen, die uns IT-Sicherheitsverantwortliche, Datenschutzbeauftragte und Einkaufsabteilungen am häufigsten stellen. Sie dient der Information; maßgeblich sind unsere AGB und die mit Ihnen geschlossene Vereinbarung zur Auftragsverarbeitung (AVV).

## 1. Rollen und Vertragsgrundlagen

### In welcher Rolle verarbeitet reteach personenbezogene Daten?

Sie sind Verantwortlicher im Sinne der DSGVO, wir sind Ihr Auftragsverarbeiter (Art. 28 DSGVO). Wir verarbeiten personenbezogene Daten ausschließlich im Auftrag und nach Ihrer Weisung. Der Abschluss einer AVV ist daher zwingend erforderlich und Voraussetzung für die Nutzung.

### Wie schließen wir die AVV ab?

Die AVV kann elektronisch im Kundenkonto abgeschlossen werden (Einstellungen > Rechtliches). Den Mustertext stellen wir vorab zum Download bereit. Unsere AVV ist ein Standard-Vertragswerk, das für alle Kunden gilt, sorgfältig geprüft und bei mehreren hundert Kunden im Einsatz ist.

### Können wir eine individuelle AVV abschließen?

Ja. Da jede Änderung unserer AVV und ihrer Anlagen anschließend in jeder individuell vereinbarten Fassung nachgeführt und überwacht werden muss, ist dies mit erheblichem Aufwand verbunden. Wir berechnen daher eine einmalige Aufwandsentschädigung von 250,- EUR netto für die Prüfung sowie eine jährliche Handlingpauschale von 500,- EUR netto.

## 2. Wo liegen Ihre Daten?

### Wo wird die Plattform betrieben?

Die reteach-Plattform wird auf Amazon Web Services in der Region eu-central-1 (Frankfurt am Main, Deutschland) betrieben. Die Anwendungen laufen containerisiert auf Kubernetes; der Datei-Speicher wird über AWS S3 mit serverseitiger Verschlüsselung bereitgestellt.

### Welche Unterauftragnehmer setzen Sie ein?

Die folgende Übersicht zeigt die aktuell eingesetzten Unterauftragnehmer. Die jeweils gültige Liste ist Bestandteil der AVV (Anlage 2) und in Ihrem Kundenkonto unter Einstellungen > Rechtliches einsehbar. Über Änderungen informieren wir Sie vier Wochen im Voraus; Sie können aus einem wichtigen datenschutzrechtlichen Grund widersprechen.

| Dienstleister           | Zweck                                                                              | Verarbeitungsort                 | Grundlage                   |
|-------------------------|------------------------------------------------------------------------------------|----------------------------------|-----------------------------|
| Amazon Web Services     | Cloud-Infrastruktur, Datenbank, Datei-Speicher, E-Mail-Versand                     | Frankfurt am Main (eu-central-1) | DPF, hilfsweise SCC         |
| BunnyWay d.o.o. (Bunny) | Videohosting und Auslieferung über CDN                                             | Ljubljana, Slowenien (EU)        | EU – kein Drittlandtransfer |
| Streamdiver GmbH        | Videoverarbeitung und -hosting                                                     | Österreich (EU)                  | EU – kein Drittlandtransfer |
| Datadog, Inc.           | Betriebsüberwachung und Fehleranalyse; Protokolldaten werden nach 7 Tagen gelöscht | EU                               | EU – kein Drittlandtransfer |
| Mixpanel, Inc.          | Analyse der Produktnutzung; nur pseudonyme Nutzer-ID,                              | Eemshaven, NL (EU)               | EU – kein Drittlandtransfer |

| Dienstleister           | Zweck                                                                    | Verarbeitungsort | Grundlage                   |
|-------------------------|--------------------------------------------------------------------------|------------------|-----------------------------|
|                         | keine E-Mail oder IP                                                     |                  |                             |
| Kombo Technologies GmbH | Schnittstellen zu HR-Systemen (nur bei Nutzung der HRIS-Synchronisation) | Berlin (EU)      | EU – kein Drittlandtransfer |
| Rustici Software, LLC   | SCORM-Verarbeitung und -hosting (nur bei Nutzung von SCORM)              | USA              | DPF, hilfsweise SCC         |
| Stripe, Inc.            | Zahlungsabwicklung (nur bei Nutzung des eCommerce-Moduls)                | USA / EU         | DPF, hilfsweise SCC         |

### Verlassen Daten die EU?

Im Regelbetrieb der Plattform verarbeiten sämtliche Unterauftragnehmer ausschließlich in der EU; ein Drittlandtransfer findet nicht statt. Eine Verarbeitung außerhalb der EU ist nur möglich, wenn Sie ein optionales Modul oder eine optionale Funktion nutzen, für die in Anlage 2 Abschnitt B der AVV ein zusätzlicher Unterauftragnehmer ausgewiesen ist – derzeit bei Nutzung von SCORM (Rustici Software, USA), des eCommerce-Moduls (Stripe, USA) oder des Moduls Phishing Awareness (Phishing Tackle, Vereinigtes Königreich). Für Übermittlungen in Drittländer stützen wir uns auf den jeweiligen Angemessenheitsbeschluss der EU-Kommission, hilfsweise auf die Standardvertragsklauseln.

### Was passiert, wenn ein Angemessenheitsbeschluss wegfällt?

Unsere AVV sieht dafür ausdrücklich vor: Entfällt ein Angemessenheitsbeschluss, auf den sich eine Übermittlung stützt, gelten für diese Übermittlung ohne weiteres die Standardvertragsklauseln. Wir informieren Sie unverzüglich und ergreifen die erforderlichen Maßnahmen. Sie müssen also nicht auf eine Vertragsanpassung warten.

### Haben Sie Transfer Impact Assessments durchgeführt?

Ja. In Anwendung von Klausel 14 der Standardvertragsklauseln haben wir für die betroffenen Unterauftragnehmer Transfer Impact Assessments (TIA) durchgeführt. Diese stellen wir Ihnen auf Anfrage zur Verfügung.

### Wie funktioniert die Videoauslieferung über das CDN?

Videos werden über ein Content Delivery Network mit Serverstandorten in Europa ausgeliefert. Die Anonymisierung der IP-Adressen in den Zugriffsprotokollen ist aktiviert; es werden ausschließlich Metadaten der Anfrage protokolliert (Zeitstempel, URL, Status, anonymisierte IP).

## 3. Welche Daten werden verarbeitet?

### Welche Daten benötigt reteach zwingend?

Für den Betrieb der Lernplattform benötigen wir technisch nur einen Benutzernamen oder eine E-Mail-Adresse sowie ein Passwort. Weitere Stammdaten speichern wir nur, wenn Sie oder Ihre Mitarbeitenden sie eingeben.

### Welche Daten entstehen bei der Nutzung?

Lernaktivität (durchgeführte Aktivitäten, Zeitpunkte), Teilnahme-, Abschluss- und Zertifikatsdaten sowie – bei Nutzung des eCommerce-Moduls – Zahlungsdaten.

### Nutzen Sie unsere Daten zur Verbesserung Ihres Produkts?

Nur in anonymisierter und aggregierter Form. Unsere AVV erlaubt uns ausdrücklich, personenbezogene Daten zu anonymisieren und die daraus entstehenden aggregierten Daten für Statistik, Benchmarking, Fehleranalyse und Produktverbesserung zu nutzen. Personenbezogene Daten oder vertrauliche Informationen werden dabei weder offengelegt noch für Dritte sichtbar.

Für die Analyse der Produktnutzung setzen wir Mixpanel ein. Übermittelt wird ausschließlich eine pseudonyme Nutzerkennung – weder Name noch E-Mail-Adresse noch IP-Adresse. Für Betriebsüberwachung und Fehleranalyse setzen wir Datadog ein. Personenbezogene Daten werden aus den Protokolldaten herausgefiltert, soweit dies technisch möglich ist; ein vollständiger Ausschluss lässt sich insbesondere bei API-Protokollen nicht garantieren. Die Protokolldaten werden daher konsequent nach sieben Tagen gelöscht. Beide Dienste verarbeiten ausschließlich in der EU und sind nach ISO 27001 und SOC 2 Type II zertifiziert.

### Setzen Sie Cookies?

Auf der Ausgabeseite Ihrer Academy setzen wir ausschließlich technisch notwendige Cookies. Binden Sie eigene Trackingdienste ein, können weitere Cookies gesetzt werden; das liegt in Ihrer Verantwortung.

## 4. Sicherheit

### Welche technischen und organisatorischen Maßnahmen setzen Sie um?

Wir betreiben ein Informationssicherheits-Managementsystem (ISMS), das sich an ISO 27001 orientiert und jährlich durch die Geschäftsführung überprüft wird. Die wesentlichen Maßnahmen:

- **Verschlüsselung:** AES-256 serverseitig über AWS KMS (at rest), TLS 1.2 oder höher für alle Übertragungen (in transit); HTTPS wird erzwungen.
- **Zugriffskontrolle:** Multi-Faktor-Authentifizierung für alle geschäftskritischen Systeme, Least Privilege und Need-to-know, regelmäßige Rechteprüfung, sofortiger Entzug beim Offboarding, verpflichtender Passwort-Manager.
- **Endgeräte:** ausschließlich Firmengeräte, zentral über MDM verwaltet, Festplattenverschlüsselung, Endpoint Protection; BYOD ist nicht gestattet.
- **Softwareentwicklung:** Code Reviews durch mindestens zwei Engineers vor Produktivsetzung, jährliche externe Penetrationstests, kritische Sicherheitsupdates innerhalb von 24 Stunden.
- **Backup und Wiederherstellung:** Point-in-Time-Recovery (RPO unter 10 Minuten), tägliche verschlüsselte Backups für 180 Tage, Recovery-Tests alle 90 Tage, RTO unter 4 Stunden.
- **Schulung:** Informationssicherheitsschulung bei Einstellung und danach jährlich, ergänzt durch laufende Phishing-Simulationen.

### Wie ist die Mandantentrennung umgesetzt?

Die Trennung erfolgt mehrstufig. 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- und mandantenbezogene Unique-Constraints auf Datenbankebene die Integrität und verhindern Kollisionen zwischen Mandanten.

### Wie reagieren Sie auf Sicherheitsvorfälle?

Wir verfügen über einen formalen Incident-Response-Plan mit Severity-Klassifikation (S1–S4), definierten Reaktionszeiten und Eskalationswegen. Bei einem bestätigten Vorfall mit Auswirkung auf Kundendaten erfolgt die Erstreaktion innerhalb von 30 Minuten. Betroffene Kunden benachrichtigen wir unverzüglich, damit Sie Ihre Meldepflicht nach Art. 33 DSGVO (72 Stunden) erfüllen können. Sicherheitslücken können jederzeit an [sicherheit@reteach.com](mailto:sicherheit@reteach.com) gemeldet werden.

### Sind Sie nach ISO 27001 zertifiziert?

Unser ISMS orientiert sich an ISO 27001; eine Zertifizierung besteht derzeit nicht. Unsere Kerninfrastruktur ist zertifiziert: AWS Frankfurt verfügt über ISO 27001:2022, SOC 2 Type II, CSA STAR und PCI-DSS. Die Zertifikate unserer Unterauftragnehmer legen wir Ihnen auf Anfrage vor.

## 5. Prüfungsrechte, Löschung und Aufbewahrung

### **Können wir reteach auditieren?**

Ja. Die Prüfung erfolgt gestuft: zunächst durch Vorlage von Dokumentationen, Zertifikaten und Nachweisen, sodann durch Fernprüfung (z. B. Fragebogen oder Videokonferenz). Reicht dies zur Klärung nicht aus, ist eine Prüfung vor Ort in unseren Geschäftsräumen möglich. Da wir keine eigenen Rechenzentren betreiben, legen wir für unsere Unterauftragnehmer deren Nachweise und Zertifikate vor.

### **Wie lange werden Daten gespeichert?**

Grundsätzlich für die Dauer des Vertragsverhältnisses. Nach dessen Beendigung geben wir die Daten nach Ihrer Weisung zurück oder löschen sie, soweit keine gesetzliche Aufbewahrungspflicht besteht.

### **Wie unterstützen Sie uns bei Betroffenenrechten?**

Wenden sich betroffene Personen an uns, leiten wir das Anliegen unverzüglich an Sie weiter und beantworten es nicht selbst – Sie bleiben als Verantwortlicher zuständig. Bei Auskunft, Berichtigung, Einschränkung und Löschung unterstützen wir Sie mit den erforderlichen technischen und organisatorischen Maßnahmen.

## **6. Anbieterwechsel (EU Data Act)**

### **Was passiert, wenn wir zu einem anderen Anbieter wechseln möchten?**

Sie können jederzeit mit einer Frist von zwei Monaten kündigen, um zu einem anderen Dienst oder in eine eigene Infrastruktur zu wechseln. Danach beginnt eine Übergangsfrist von 30 Tagen, in der wir Sie beim Wechsel unterstützen und der Zugang erhalten bleibt. Ihre Daten stellen wir in einem gängigen, strukturierten und maschinenlesbaren Format bereit. Für den Wechsel und den Datenexport erheben wir kein Entgelt.

## **Kontakt**

Für das Modul Phishing Awareness stellen wir ein eigenes Datenschutz-FAQ bereit.

Datenschutz: [datenschutz@reteach.com](mailto:datenschutz@reteach.com)

Sicherheit und Meldung von Schwachstellen: [sicherheit@reteach.com](mailto:sicherheit@reteach.com)

AGB, AVV und archivierte Fassungen: <https://www.reteach.com/agb/>