Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (Art. 28 DSGVO)

Muster für NormProof, Stand 18. September 2026

Auftragsverarbeiter	Sascha Manke, Westerbachstraße 50, 60489 Frankfurt am Main (NormProof)
Verantwortlicher	der Firmenkunde, im Folgenden „Kunde"
Anlass	Das erste echte Firmenkonto entsteht am 18.09.2026
Verfasser	Stab · Recht. **Kein Anwalt. Dies ist keine Rechtsauskunft.**

Was dieses Muster ist: eine Unterlage, die dasteht, wenn ein Kunde nach einem AVV fragt, und die ein Anwalt prüfen kann, statt sie zu schreiben.

Was es nicht ist: unterschriftsreif. Vor der ersten Unterzeichnung sind die in **Teil 3** benannten Lücken zu schließen. Ein AVV, dessen Anlage die Datenarten falsch beschreibt, ist schlechter als keiner - er behauptet eine Kontrolle, die es nicht gibt.

Teil 0 · Was in diesem Dokument gemessen ist und was nicht

Gemessen am System am 18.09.2026 (Migrationen, Modelle, Ansichten, Konsolen- kommandos, Tests): sämtliche Datenarten in Anlage 2, die Angaben auf dem Nachweis, die Inhalte der öffentlichen Prüfseite, die Löschfristen in Anlage 3, das Fehlen eines Verarbeitungsverzeichnisses, und bei den Unterauftragnehmern in Anlage 5 jeweils die Zeile „gemessen".

Ebenfalls gemessen und am 18.09.2026 nachgetragen: Serverbetreiber und Standort, Anbieter des Mailversands, die Aufbewahrung der automatischen Sicherungen sowie der Zustand der Handsicherungen und der Dateirechte in Anlage 4.

Nicht gemessen, sondern ausdrücklich als offen gekennzeichnet: die Grundlage des Drittlandtransfers zu Cloudflare und die Frage in Teil 1, ob der Nachweis in eigener Verantwortlichkeit oder im Auftrag verarbeitet wird. **Diese Punkte sind in Teil 3 aufgeführt und dürfen nicht durch eine Annahme gefüllt werden.**

Teil 1 · Rollenabgrenzung. Der Teil, den Mustervorlagen falsch machen

Nicht alles, was NormProof über die Beschäftigten eines Kunden verarbeitet, ist Auftragsverarbeitung. Die Abgrenzung gehört in den Vertrag, weil sonst ein Teil der Verarbeitung ohne Rechtsgrundlage dasteht und ein anderer einer Weisung unterworfen wird, der er nicht unterworfen sein kann.

Im Auftrag des Kunden (Art. 28 DSGVO), Gegenstand dieses Vertrags: Benutzerkonto, Zugehörigkeit zur Firma, Lizenzzuweisung, Kursteilnahme,

Lernfortschritt, Prüfungsversuche, Antwortprotokoll, Zugriffsprotokolle. Der Kunde entscheidet, wer teilnimmt und zu welchem Zweck.

In eigener Verantwortlichkeit von NormProof, nicht Gegenstand dieses Vertrags: Vertrags- und Rechnungsdaten des Kunden einschließlich der handelnden Personen. Grundlage: Art. 6 Abs. 1 lit. b und lit. c DSGVO, Aufbewahrung nach § 257 HGB und § 147 AO.

> ⚠ **OFFENE FRAGE, die vor der ersten Unterzeichnung entschieden gehört:** In welcher Rolle wird der **Nachweis** verarbeitet? NormProof stellt ihn im eigenen Namen als bescheinigende Stelle aus, versieht ihn mit einer eigenen Prüfnummer und hält ihn über einen Prüflink für Dritte nachprüfbar. Das spricht für eigene Verantwortlichkeit, wie bei einer Prüfstelle. Gleichzeitig entsteht er aus Daten, die im Auftrag verarbeitet wurden.
>
> **Warum das nicht akademisch ist:** Wäre der Nachweis Auftragsverarbeitung, müsste NormProof ihn auf Weisung des Kunden löschen. Genau das darf eine bescheinigende Stelle nicht, sonst ist der Nachweis nichts wert. **Wir halten es für eigene Verantwortlichkeit, können das aber nicht verbindlich feststellen.** Bis zur Klärung steht in Anlage 3 die gemessene Tatsache, nicht die Bewertung.

Teil 2 · Vertragsklauseln

§ 1 Gegenstand und Dauer. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zu den in Anlage 1 genannten Zwecken. Die Dauer entspricht der Laufzeit des Hauptvertrags.

§ 2 Weisungsgebundenheit (Art. 28 Abs. 3 lit. a). Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Kunden. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies mit und darf die Ausführung aussetzen.

§ 3 Vertraulichkeit (lit. b). Die mit der Verarbeitung befassten Personen sind zur Vertraulichkeit verpflichtet. Anzahl und Funktion siehe Anlage 4.

§ 4 Sicherheit der Verarbeitung (lit. c, Art. 32). Es gelten die Maßnahmen in Anlage 4.

§ 5 Unterauftragsverarbeiter (lit. d, Art. 28 Abs. 2 und 4). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 5 benannt und werden vom Kunden genehmigt. Weitere setzt der Auftragsverarbeiter nur nach vorheriger Information ein; der Kunde kann binnen zwei Wochen widersprechen. **Berichtigt der Auftragsverarbeiter eine Angabe in den Anlagen, die den Umfang der Verarbeitung, die Datenarten oder die Unterauftragsverarbeiter betrifft, teilt er dies dem Kunden mit; das vorstehende Widerspruchsrecht gilt entsprechend und beginnt mit der Mitteilung.**

§ 6 Unterstützung bei Betroffenenrechten (lit. e, Art. 12 bis 22). Der Auftragsverarbeiter unterstützt den Kunden bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch. Anfragen betroffener Personen leitet er unverzüglich an den Kunden weiter und beantwortet sie nicht selbst.

§ 7 Unterstützung bei weiteren Pflichten (lit. f, Art. 32 bis 36). Der Auftragsverarbeiter unterstützt bei Sicherheit der Verarbeitung, Meldung von Verletzungen und Datenschutz-Folgenabschätzung. **Er informiert den Kunden unverzüglich, spätestens binnen 24 Stunden nach Kenntnis, über jede Verletzung des Schutzes personenbezogener Daten.**

§ 8 Löschung und Rückgabe (lit. g). Nach Beendigung löscht der Auftragsverarbeiter die im Auftrag verarbeiteten Daten nach Anlage 3, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. **Der Kunde kann vor der Löschung einen Export verlangen.**

§ 9 Nachweise und Kontrolle (lit. h). Der Auftragsverarbeiter stellt die zum Nachweis erforderlichen Informationen bereit und ermöglicht Überprüfungen nach angemessener Vorankündigung.

§ 10 Verarbeitung außerhalb der EU. Eine Verarbeitung in einem Drittland erfolgt nur, soweit in Anlage 5 benannt und auf einer Grundlage nach Art. 44 ff. DSGVO.

Anlage 1 · Gegenstand, Art, Zweck und Dauer

Gegenstand	Betrieb einer Lernplattform für gesetzlich vorgeschriebene Unterweisungen und Ausstellung der zugehörigen Nachweise
Art der Verarbeitung	Erheben, Speichern, Auswerten von Lernfortschritt und Prüfungsergebnissen, Erzeugen von Nachweisdokumenten, Protokollieren von Zugriffen
Zweck	Durchführung der vom Kunden beauftragten Unterweisungen und Belegführung für dessen eigene Dokumentationspflicht, unter anderem nach § 12 ArbSchG
Betroffene	Beschäftigte des Kunden, die einen Kurs zugewiesen bekommen; Personen mit Verwaltungsrechten im Firmenkonto
Dauer	Laufzeit des Hauptvertrags, danach nach Anlage 3

Anlage 2 · Datenarten. Vollständig am System gemessen

Je Beschäftigtem des Kunden können folgende Daten entstehen. Die Tabellennamen sind mitgenannt, damit der Kunde jede Zeile nachprüfen kann.

Datenart	Einzelangaben	Tabelle
Kontodaten	Name, E-Mail-Adresse, Zeitpunkt der E-Mail-Bestätigung, Passwort als Hashwert, Anmelde-Merkmal	`users`
Zugehörigkeit	Zuordnung zum Firmenkonto, Rolle	`org_user`
Lizenzzuweisung	zugewiesener Kurs, Startzeitpunkt, Ablaufzeitpunkt	`course_licenses`
Kursteilnahme	Kurs, Status, Fortschritt in Prozent, Abschlusszeitpunkt	`enrollments`

Datenart	Einzelangaben	Tabelle
Prüfungsergebnis je Kapitel	Anzahl Fragen, Anzahl richtiger Antworten, fehlerfrei ja/nein, **Nummer des Versuchs**	`chapter_results`
Antwortprotokoll je Frage	**welche Antwortoptionen gezeigt wurden, welche die Person gewählt hat, richtig oder falsch**	`chapter_answers`
Nachweis	Kurs, Prüfnummer, Ausstellungsdatum, Gültigkeitsdatum, Prüftoken	`certificates`
Zugriffsprotokoll	Handlung, Zeitpunkt, **IP-Adresse**, betroffene Person, betroffenes Dokument	`access_logs`
Sitzungsdaten	**IP-Adresse, Browserkennung**, Zeitpunkt der letzten Aktivität	`sessions`
Nachrichten	Inhalte, sofern die Person Support oder Teamnachrichten nutzt	`messages`, `tickets`, `ticket_messages`
Praktischer Teil	Ergebnis einer Praxisprüfung, sofern der Kurs einen vorsieht	`praxispruefungen`

> **Auf das Antwortprotokoll ist der Kunde ausdrücklich hinzuweisen.** Es ist nicht dasselbe wie ein Kursergebnis: Es lässt erkennen, welche einzelne Frage eine namentlich bekannte Person falsch beantwortet hat. **Das ist ein Leistungs- und Verhaltensdatum.** Ob und wie der Kunde darauf zugreifen darf, richtet sich nach seinem eigenen Beschäftigtendatenschutz, insbesondere § 26 BDSG und einer etwaigen Mitbestimmung. **Wir stellen es fest, wir bewerten es nicht.**

Was der Nachweis trägt, gemessen an der Druckansicht: Name der Person, Kurstitel, Art des Nachweises, Wissensstand, Ausstellungsdatum, Prüfnummer, die Nachweiszeile und einen Prüflink als QR-Code. **Nicht darauf: die E-Mail-Adresse und nicht der Name des Arbeitgebers.**

Was die öffentliche Prüfseite zeigt: dieselben Angaben wie der Nachweis. Der Prüflink enthält ein 40 Zeichen langes Zufallsmerkmal und ist ohne dieses nicht erreichbar. **Wer den Nachweis in der Hand hat, kann ihn prüfen; wer ihn**

nicht hat, findet nichts.

Keine besonderen Kategorien nach Art. 9 DSGVO. Gesundheitsdaten, Gewerkschaftszugehörigkeit, biometrische Daten werden nicht verarbeitet. Es gibt kein Feld dafür.

Anlage 3 · Löschung und Aufbewahrung. Am System gemessen

Gebaute Fristen (Konsolenkommando `AccountLifecycle`, `PruneTrials`):

Auslöser	Frist	Was geschieht
Rechnung überfällig	14 Tage nach Mahnung	Ankündigung der Sperre
Firmenkonto gesperrt	10 Monate	Löschwarnung mit Hinweis auf Export
Firmenkonto gesperrt	**12 Monate**	**Bereinigung:** Lizenzen, Kursteilnahmen und damit Prüfungsergebnisse und Antwortprotokolle, Einladungen, Nachrichten, Dokumentfreigaben und Mitgliedschaften werden gelöscht
kein Login	**24 Monate**, dann Warnung und 30 Tage	Löschung des Benutzerkontos
Testzugang abgelaufen	Ablauf plus Gnadenfrist	Löschung

> **Zwei Eigenschaften dieser Fristen, die ein Kunde kennen muss:**
>
> **(1)** Bei der Bereinigung nach 12 Monaten bleiben **Bestellungen, die Firmenzeile und die Benutzerdaten** erhalten. Gelöscht werden die Kursdaten. Grund für den Rest sind die handels- und steuerrechtlichen Aufbewahrungspflichten.

(2) □□ Der Nachweis wird von dieser Bereinigung nicht erfasst. Er hängt technisch am Benutzerkonto, nicht an der Kursteilnahme, und überlebt damit die Kursdaten, aus denen er entstanden ist. **Das ist für eine Bescheinigung sachgerecht, ist aber eine andere Frist als die der übrigen Daten, und es hängt an der offenen Rollenfrage aus Teil 1.**

Löschung auf Weisung des Kunden ist außerhalb dieser Fristen möglich. **Für den Nachweis gilt das nur, soweit die Rollenfrage aus Teil 1 geklärt ist.**

Wann eine Löschung in den Sicherungen vollzogen ist

Beide Teile werden genannt, weil es zwei gibt.

Automatische Sicherungen. Nächtlich, seit dem 24. August 2026. Aufbewahrt werden die Stände der letzten sieben Tage sowie die letzten fünf Sonntage. Ältere werden entfernt; der Lauf protokolliert das. **Eine Löschung ist in diesen Sicherungen daher spätestens fünf Wochen nach ihrer Ausführung vollzogen.**

Von Hand angelegte Sicherungen. Neben den automatischen Ständen können einzelne Sicherungen von Hand entstehen, etwa vor einer Umstellung. Für sie gilt seit dem 20. September 2026 eine Aufbewahrungsfrist von **30 Tagen**; ein eigener Lauf entfernt sie täglich nach Ablauf dieser Frist und protokolliert das. **Eine Löschung ist in diesen Sicherungen daher spätestens 30 Tage nach ihrer Ausführung vollzogen.**

Anlage 4 · Technische und organisatorische Maßnahmen (Art. 32)

Gemessen:

- **Passwörter** werden nicht im Klartext gespeichert, sondern als Hashwert.
- **Zwei-Faktor-Anmeldung** ist vorhanden; Sicherungs-E-Mail und Bestätigungscode sind im Konto einstellbar.
- **Rollen- und Rechtetrennung:** Zugriff auf Daten eines Firmenkontos ist an die Mitgliedschaft und die Rolle gebunden; ein gesperrtes Firmenkonto wird durch eine eigene Prüfschicht am Zugriff gehindert.
- **Protokollierung:** Zugriffe auf Dokumente und Nachweise werden mit Handlung, Zeitpunkt, handelnder Person und IP-Adresse protokolliert.
- **Übersetzung und KI-Unterstützung laufen im eigenen Netz.** Ein Test hält fest, dass die entsprechenden Endpunkte im eigenen Netz liegen und dass für Anbieter wie DeepL, OpenAI, Anthropic, Azure oder Google Translate **keine Konfigurationsfelder existieren** - nicht „keiner konfiguriert", sondern „das Feld gibt es nicht". Grundlage ist eine Vorgabe vom 07.09.2026: keine ausländischen Server.

Sicherungen. Sicherungen der Datenbank werden **unverschlüsselt** abgelegt. Der Schutz besteht in der Zugriffsbeschränkung, und zwar auf zwei verschiedenen Ebenen:

- **Automatische Sicherungen** liegen in einem eigenen Verzeichnis, das nur mit Systemverwalterrechten lesbar ist.
- **Von Hand angelegte Sicherungen** liegen im Ausgangsverzeichnis des Systemverwalters, das gegen jeden anderen Zugriff gesperrt ist. **Die Dateien darin sind seit dem 20. September 2026 zusätzlich nur für den Systemverwalter lesbar**; zuvor trugen einzelne allgemein lesbare Rechte.

  ⚠ **Nicht gemessen und vor der Unterzeichnung zu ergänzen:** Wiederherstellungs- zeiten, Anzahl und Funktion der auf Vertraulichkeit verpflichteten Personen, physische Zugangssicherung des Serverstandorts.

Anlage 5 · Unterauftragsverarbeiter

Dienst	Zweck	Daten	Stand

Cloudflare, Inc.	Auslieferung der Seiten, Namensauflösung, Verbindungsschutz	**alle übertragenen Inhalte** sowie Verbindungsdaten einschließlich der IP-Adresse. Die verschlüsselte Verbindung endet bei Cloudflare	**gemessen am 21.09.2026** (beide Domains über Cloudflare, TLS endet dort). Auftragsverarbeitung. □□ **Sitz in den Vereinigten Staaten; die Grundlage nach Art. 44 ff. DSGVO ist zu benennen**
Hetzner Online GmbH, Nürnberg, Deutschland	Betrieb der Anwendung und der Datenbank auf einem gemieteten virtuellen Server	alle Daten aus Anlage 2	**gemessen** (Virtualisierung, Board-Kennung, Reverse-DNS und Netzzuordnung deckungsgleich). Auftragsverarbeitung. **Standort Deutschland, kein Drittland**
IONOS SE	Zustellung von Einladungen, Erinnerungen, Benachrichtigungen	Name, E-Mail-Adresse, Nachrichteninhalt	**gemessen:** SMTP an `smtp.ionos.de`, Port 587, TLS. Auftragsverarbeitung
Sprachausgabe (edge-tts)	Vertonung der Kurstexte	**keine personenbezogenen Daten.** Übergeben wird ausschließlich der Kurstext	**gemessen.** Kein Unterauftragsverarbeiter im Sinne dieses Vertrags. ⚠ **Hausinterner Hinweis, siehe Teil 3**
Übersetzung, KI-Unterstützung	Sprachfassungen, Assistent	Kurstexte, Nutzertexte	**gemessen: eigenes Netz, kein externer Anbieter.** Kein Unterauftragsverarbeiter

Teil 3 · Was vor der ersten Unterzeichnung fehlt

Fünf Punkte. Keiner davon ist eine Rechtsfrage, vier sind in einer halben Stunde zu klären.

1. **Ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO existiert nicht.** Gesucht und nicht gefunden; vorhanden sind lediglich zwei DSGVO-Prüfberichte zu einzelnen Funktionen. **Art. 30 gilt unabhängig von diesem Vertrag, und Abs. 2 verlangt es auch vom Auftragsverarbeiter selbst.** Die Anlagen 1 bis 5 dieses Musters enthalten den größeren Teil des Inhalts, den ein solches Verzeichnis braucht.
2. **Erledigt am 18.09.2026:** Serverbetreiber (Hetzner, Nürnberg) und Mailanbieter (IONOS) sind gemessen und in Anlage 5 eingetragen.
3. **Erledigt am 20.09.2026:** Die von Hand angelegten Sicherungen haben eine Aufbewahrungsfrist von 30 Tagen, der Bereinigungslauf arbeitet täglich. Damit ist die Löschzusage aus § 8 für beide Sicherungsbestände eingehalten.
4. **Grundlage für den Drittlandtransfer zu Cloudflare benennen.** Der Transfer ist seit dem 21.09.2026 gemessen und keine offene Frage mehr: beide Domains laufen über Cloudflare, die verschlüsselte Verbindung endet dort. In Betracht kommen der Angemessenheitsbeschluss zum EU-US Data Privacy Framework oder die Standardvertragsklauseln aus dem Vertrag mit Cloudflare. **Welche gilt, ist eine Tatsachenfrage und hängt an Punkt 2.**
5. **Die Rollenfrage aus Teil 1 entscheiden:** Nachweis in eigener Verantwortlichkeit oder im Auftrag. Sie entscheidet, ob ein Kunde die Löschung eines Nachweises verlangen kann.

Ein hausinterner Punkt, der nicht in den Vertrag gehört, aber hierher: Die Sprachausgabe über edge-tts ist ein Dienst außerhalb Deutschlands. Sie verarbeitet keine personenbezogenen Daten, ist also für diesen Vertrag ohne Bedeutung. **Sie fällt aber unter die Vorgabe vom 07.09.2026 und wird von dem Test, der diese Vorgabe absichert, nicht erfasst** - der prüft die Endpunkte für Übersetzung und Assistent, nicht die Vertonung. Das ist eine Entscheidung für die Leitung, keine Rechtsfrage.

Drucken / als PDF speichern