



ExamLab

REPETITORIUM · RECHT · EXAMEN

RECHTSDOKUMENT · DATENSCHUTZ

Datenschutzerklärung

Verarbeitung personenbezogener Daten nach DSGVO, TDDDG und EU-AI-Act

DSGVO · TDDDG · ART. 22 DSGVO · KI-VO

DOKUMENT

EL-DS-2026-06

STAND

Juni 2026

KAPITEL

Datenschutz

NORMEN

Art. 5, 6, 8, 9, 10, 12–22, 28, 30, 32, 35, 44–49, 77 DSGVO · §§ 38, 147 AO · § 257 HGB · § 25 TDDDG · § 7 Abs. 2 UWG · Art. 22, 50 KI-VO (VO (EU) 2024/1689) · § 44b UrhG (nur urheberrechtlich, siehe § 4.13)

ROUTE

/legal/datenschutz

DOKUMENTENKOPF**ExamLab — KI-gestützte Jura-Lernplattform**

Feld	Angabe
Dokument	Datenschutzerklärung
Dok-Nr.	EL-DS-2026-06
Stand	Juni 2026
Anbieter / Verantwortlic her	Yusuf Yeneroglu, Einzelunternehmer (Kleinunternehmer i.S.d. § 19 UStG)
Anschrift	Rösratherstraße 44, 51107 Köln, Deutschland
Kontakt	info@exam-lab.de · Datenschutz: datenschutz@exam-lab.de · Support: support@exam-lab.de · Tel. +49 151 70 54 36 75 (Mo–Fr 10:00–12:00 Uhr)
Plattform	exam-lab.de
Einschlägige Normen	Art. 5, 6, 8, 9, 10, 12–22, 28, 30, 32, 35, 44–49, 77 DSGVO · §§ 38, 147 AO · § 257 HGB · § 25 TDDDG · § 7 Abs. 2 UWG · Art. 22, 50 KI-VO (VO (EU) 2024/1689) · § 44b UrhG (nur urheberrechtlich, siehe § 4.13)

RECHTSDOKUMENT

§ 1 Allgemeines und Geltungsbereich

- 1.1** Diese Datenschutzerklärung informiert über Art, Umfang und Zweck der Verarbeitung personenbezogener Daten auf der unter exam-lab.de erreichbaren Plattform sowie über die Rechte der Nutzer nach der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG).
- 1.2** Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist Yusuf Yeneroglu (Anschrift wie oben). Ein Vertreter nach Art. 27 DSGVO ist nicht zu benennen, da der Verantwortliche in der Union niedergelassen ist.
- 1.3** Ein Datenschutzbeauftragter ist nicht bestellt, weil die Voraussetzungen des § 38 Abs. 1 BDSG nicht vorliegen: In der Regel sind weniger als zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, und es findet keine Verarbeitung statt, die nach Art. 37 Abs. 1 DSGVO eine Bestellung erforderlich macht. In Datenschutzfragen erreichst du den Verantwortlichen unmittelbar unter datenschutz@exam-lab.de.
- 1.4** Das Angebot richtet sich an volljährige Nutzer sowie an Minderjährige, die das sechzehnte Lebensjahr vollendet haben. Soweit eine Verarbeitung auf einer Einwilligung beruht (etwa bei nicht zwingend erforderlichen Cookies oder beim Newsletter) und der Nutzer das sechzehnte Lebensjahr noch nicht vollendet hat, ist diese Einwilligung nur mit Zustimmung der Sorgeberechtigten wirksam (Art. 8 DSGVO).
- 1.5** ExamLab ist ein kostenpflichtiges Angebot (7-Tage-Trial, anschließend Abonnement, Bestellung über die Schaltfläche „Kostenpflichtig bestellen“). Der kostenpflichtige Vertrag wird über Art. 6 Abs. 1 lit. b DSGVO abgewickelt. Soweit ein Minderjähriger das Angebot kostenpflichtig nutzen möchte, bedarf der zugrunde liegende Vertrag nach §§ 104 ff., 107 BGB der Einwilligung bzw. Genehmigung der gesetzlichen Vertreter; ohne deren Zustimmung darf das kostenpflichtige Angebot nicht abgeschlossen werden. Diese Klarstellung dient der Vermeidung eines Widerspruchs zwischen Zielgruppe und Geschäftsmodell und berührt die datenschutzrechtliche Altersgrenze des Art. 8 DSGVO (16 Jahre für einwilligungsbasierte Dienste) nicht.

RECHTSDOKUMENT

§ 2 Begriffsbestimmungen

Es gelten die Begriffsbestimmungen des Art. 4 DSGVO. Insbesondere bedeutet:

- **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- **Verarbeitung** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten.
- **Auftragsverarbeiter** ist eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 28 DSGVO).
- **Besondere Kategorien personenbezogener Daten** sind die in Art. 9 Abs. 1 DSGVO genannten Daten (etwa Gesundheits-, religiöse oder politische Daten). Daten über strafrechtliche Verurteilungen und Straftaten richten sich nach Art. 10 DSGVO.

RECHTSDOKUMENT

§ 3 Rechtsgrundlagen der Verarbeitung

Wir verarbeiten personenbezogene Daten auf folgenden Rechtsgrundlagen:

- **Art. 6 Abs. 1 lit. a DSGVO** — Einwilligung; bei besonderen Kategorien zusätzlich Art. 9 Abs. 2 lit. a DSGVO (ausdrückliche Einwilligung).
- **Art. 6 Abs. 1 lit. b DSGVO** — Erfüllung des Nutzungsvertrages oder vorvertraglicher Maßnahmen.
- **Art. 6 Abs. 1 lit. c DSGVO** — Erfüllung gesetzlicher Verpflichtungen (insbesondere handels- und steuerrechtliche Aufbewahrung).
- **Art. 6 Abs. 1 lit. f DSGVO** — Wahrung berechtigter Interessen, soweit Interessen der betroffenen Person nicht überwiegen. Die jeweils maßgebliche Interessenabwägung haben wir bei der betreffenden Verarbeitungstätigkeit dokumentiert; sie kann unter datenschutz@exam-lab.de angefordert werden.
- **Art. 49 Abs. 1 lit. a DSGVO** — ausdrückliche, gesonderte Einwilligung in die nur gelegentliche Übermittlung an Anbieter in unsicheren Drittländern (China), siehe § 7.
- **§ 25 Abs. 1 und Abs. 2 TDDDG** — Speicherung von Informationen auf dem Endgerät bzw. Zugriff darauf (Cookies, vergleichbare Technologien), siehe § 5.

RECHTSDOKUMENT

§ 4 Verarbeitungstätigkeiten im Einzelnen

Hinweis zur Bereitstellungspflicht (Art. 13 Abs. 2 lit. e DSGVO): Soweit eine Verarbeitungstätigkeit als „Bereitstellung erforderlich“ gekennzeichnet ist, ist die Angabe der Daten für den Abschluss bzw. die Durchführung des Nutzungs- oder Zahlungsvertrages erforderlich. Werden diese Daten nicht bereitgestellt, kann der jeweilige Vertrag nicht geschlossen oder die jeweilige Funktion nicht erbracht werden. Eine darüber hinausgehende gesetzliche Pflicht zur Bereitstellung besteht nicht; die Eingabe von Lerninhalten (z. B. Klausurtexten) ist stets freiwillig.

4.1 Nutzerkonto und Authentifizierung

Daten: E-Mail-Adresse, Passwort-Hash, Profildaten, Studienphase.

Zweck: Bereitstellung des Accounts, Vertragsabwicklung.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO.

Bereitstellung: E-Mail-Adresse und Passwort sind für die Vertragsdurchführung erforderlich; ohne sie kann kein Konto angelegt werden (Art. 13 Abs. 2 lit. e DSGVO).

Speicherdauer: bis zur Accountlöschung, anschließend dreißig Tage Soft-Delete (§ 9).

Beim Login werden Zeitstempel, eine gekürzte bzw. pseudonymisierte IP-Adresse und Geräte-Informationen erfasst, um unbefugte Zugriffe zu erkennen (Art. 6 Abs. 1 lit. f DSGVO; berechtigtes Interesse an IT-Sicherheit). Eine vollständige Anonymisierung findet hier nicht statt, weil die zur Missbrauchserkennung erforderliche Zuordenbarkeit erhalten bleiben muss; die IP wird daher gekürzt und nach Ablauf der Sicherheitsfristen gemäß § 4.11 vollständig anonymisiert. Token für die Zwei-Faktor-Authentifizierung werden verschlüsselt gespeichert.

4.2 Single-Sign-On (Google, Apple)

Daten: OAuth-Sub-ID, E-Mail-Adresse, Anzeigenname.

Zweck: Optionales Login über Drittanbieter.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragsdurchführung) sowie Art. 6 Abs. 1 lit. a DSGVO (freiwillige Wahl des Anmeldeverfahrens).

Empfänger / Rolle: Google Ireland Ltd. und Apple Distribution International Ltd. handeln bei der Authentifizierung als eigene Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO (nicht als Auftragsverarbeiter); für deren Verarbeitung in ihrer Rolle als Identitätsanbieter gelten deren eigene Datenschutzhinweise.

Quelle der Daten: Die genannten Daten erhalten wir vom gewählten Identitätsanbieter (Art. 14 Abs. 2 lit. f DSGVO), nachdem du dich dort angemeldet hast.

Speicherdauer: bis zur Accountlöschung oder bis zur Trennung der Verknüpfung in den Einstellungen.

4.3 Zahlungsabwicklung

Daten: Zahlungs-Token, Rechnungsdaten, Stripe-Customer-ID, Subscription-Status, gekürzte IP-Adresse.

Zweck: Vertragserfüllung, Rechnungsstellung, Buchhaltung (7-Tage-Trial, Tarifverwaltung, „Kostenpflichtig bestellen“).

Rechtsgrundlage: Art. 6 Abs. 1 lit. b und lit. c DSGVO.

Empfänger: Stripe Payments Europe Ltd. (Irland), Stripe Inc. (USA).

Bereitstellung: Die Rechnungs- und Zahlungsdaten sind für den Abschluss des kostenpflichtigen Vertrages und zur Erfüllung steuer- und handelsrechtlicher Pflichten erforderlich; ohne sie kann kein kostenpflichtiges Abonnement abgeschlossen werden (Art. 13 Abs. 2 lit. e DSGVO).

Speicherdauer: Rechnungs- und Buchhaltungsdaten zehn Jahre (§ 257 HGB, § 147 AO).

Vollständige Kreditkartendaten werden nicht von uns gespeichert, sondern unmittelbar von Stripe verarbeitet.

4.4 KI-gestützte Funktionen

Daten: vom Nutzer eingegebene Klausur- und Sachverhaltstexte, Quiz-Antworten, Karteikarten-Eingaben.

Zweck: Bereitstellung der KI-Funktionen (Examens-Coach, Sachverhalts-Lese-Trainer, Quiz-Erklärungen, Karteikarten-Generierung, Copilot).

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO; bei chinesischen Anbietern zusätzlich Art. 49 Abs. 1 lit. a DSGVO für nur gelegentliche Übermittlungen (§ 7).

Bereitstellung: Die Eingabe von Klausur- und Lerninhalten ist freiwillig; ohne Eingabe kann die jeweilige KI-Funktion lediglich nicht genutzt werden (Art. 13 Abs. 2 lit. e DSGVO).

Speicherdauer: Ergebnisse bis zur Accountlöschung in unserer Datenbank; beim KI-Anbieter höchstens dreißig Tage (§ 7).

PII-Filter (Pseudonymisierung): Vor jeder Übermittlung an einen KI-Anbieter durchläuft die Eingabe einen internen Filter, der erkennbare direkte Identifikatoren (Vor- und Nachname, E-Mail, IBAN, Anschrift, Telefonnummer) entfernt oder pseudonymisiert. Dieser Filter erfasst technisch **nur die genannten direkten Identifikatoren**. Er erkennt **keine** besonderen Kategorien nach Art. 9 DSGVO (z. B. Gesundheits-, Religions-, Sexual- oder Gewerkschaftsdaten) und **keine** strafrechtlichen Daten nach Art. 10 DSGVO, die in einem frei formulierten Sachverhaltstext enthalten sein können. Die eingesetzten Anbieter sind in § 7 aufgeführt.

Besondere Kategorien (Art. 9 DSGVO) und strafrechtliche Daten (Art. 10 DSGVO): Die Eingabefelder sind ausschließlich für **fiktive Prüfungssachverhalte** bestimmt. Bitte gib dort keine realen sensiblen Eigendaten ein (etwa Gesundheits-, Religions-, Sexual- oder Strafrechtsdaten zu deiner oder einer dritten realen Person). Wir weisen ausdrücklich darauf hin, dass der PII-Filter solche Inhalte – anders als direkte Identifikatoren – technisch nicht zuverlässig erkennen und nicht entfernen kann. Schutz erreichen wir daher vorrangig durch das Gebot, nur fiktive Sachverhalte einzugeben, durch sichtbare Hinweise an den Eingabefeldern (Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO) sowie durch die kurzen Löschfristen beim KI-Anbieter (§ 7). Soweit du dennoch besondere Kategorien nach Art. 9 Abs. 1 oder strafrechtliche Daten nach Art. 10 DSGVO mit Bezug zu einer realen Person eingibst, geschieht dies auf deine eigene Veranlassung; eine darauf gestützte Verarbeitung erfolgt allein auf Grundlage deiner durch die bewusste Eingabe erteilten ausdrücklichen Einwilligung (Art. 9 Abs. 2 lit. a DSGVO), die du jederzeit mit Wirkung für die Zukunft widerrufen kannst (Löschung des betreffenden Inhalts in deinem Konto). Da eine solche beiläufige Einwilligung in einem Freitextfeld in Granularität und Nachweisbarkeit eingeschränkt ist, empfehlen wir dringend, von der Eingabe realer sensibler Daten abzusehen.

Automatisierte Bewertung (Art. 22 DSGVO): Die KI-Klausurkorrektur erstellt eine vollautomatisierte, ausdrücklich unverbindliche Einschätzung (geschätzte Note nebst Schwächenanalyse und Lernpfad) ohne menschliche Einzelfallentscheidung. Sie stellt kein verbindliches Prüfungsergebnis dar, ersetzt keine staatliche oder universitäre Prüfungsbewertung und entfaltet keine unmittelbare rechtliche Wirkung. Wir verkennen nicht, dass nach der Rechtsprechung des EuGH (Urteil vom 07.12.2023, C-634/21 – SCHUFA) und nach der bildungsbezogenen Risikologik der KI-VO eine automatisierte Bewertung **nach ihrer tatsächlichen Wirkung** und nicht nach ihrer Bezeichnung zu beurteilen ist und dass eine notenartige Einschätzung mit Schwächenanalyse und steuerndem Lernpfad in den Schutzbereich des Art. 22 DSGVO gezogen werden kann. Aus diesem Grund verlassen wir uns nicht allein auf die Einordnung als bloße Lernhilfe, sondern räumen vorsorglich die Garantien des Art. 22 Abs. 3 DSGVO ein, unabhängig davon, ob ein Anwendungsfall des Art. 22 Abs. 1 DSGVO vorliegt:

- Du kannst die KI-Bewertung jederzeit deaktivieren (Opt-out) und ExamLab ohne automatisierte Notenschätzung nutzen.
- Du kannst auf Verlangen das **Eingreifen einer natürlichen Person** auf Seiten des Verantwortlichen erreichen, **deinen Standpunkt darlegen** und die automatisierte Einschätzung **anfechten** (Anfrage an datenschutz@exam-lab.de).
- Du kannst dich für eine verbindliche Bewertung jederzeit an deine Korrektorin bzw. deinen Korrektor oder an deine Universität wenden.

Die einbezogene Logik beruht auf einem Abgleich deiner Einsendung mit einer Musterlösung anhand juristischer Bewertungskriterien; die Note wird ankerbasiert und als Spanne ausgegeben.

KI-Transparenz (Art. 50 KI-VO): KI-gestützte Funktionen sind als solche gekennzeichnet, und KI-generierte Ausgaben werden als „KI-generiert“ dargestellt. Diese Kennzeichnung setzt die Transparenzpflicht des Art. 50 KI-VO (VO (EU) 2024/1689) um, die ab dem 02.08.2026 verbindlich gilt.

4.5 Lernfortschritt, Personalisierung und Lernplaner

Daten: Karteikarten-Reviews, Quiz-Ergebnisse, Schemata- und Rechtsprechungs-Nutzung, Zeitstempel, Lernziele.

Zweck: Anwendung des FSRS-Algorithmus (Spaced Repetition), personalisierte Lernempfehlungen sowie der Lernplaner („Magic Reorganizer“).

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO.

Speicherdauer: bis zur Accountlöschung.

Der Lernplaner („Magic Reorganizer“) arbeitet ausschließlich **regelbasiert** und setzt **keine generative KI** ein. Es findet keine Profilbildung mit rechtlicher oder ähnlich erheblicher Wirkung im Sinne des Art. 22 DSGVO statt.

4.6 Dokumentenbibliothek und eigene Dokumente

Daten: hochgeladene PDF- und Text-Inhalte, Annotationen.

Zweck: Bereitstellung der Bibliotheksfunktion.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO.

Bereitstellung: freiwillig; ohne Upload steht lediglich die Bibliotheksfunktion nicht zur Verfügung (Art. 13 Abs. 2 lit. e DSGVO).

Speicherdauer: bis zur Accountlöschung oder bis zur Löschung durch den Nutzer.

4.7 Transaktionale E-Mails

Daten: E-Mail-Adresse, Versand-Status, Bounce-Informationen.

Zweck: Verifizierung, Trial-Hinweise, Rechnungs- und Kündigungsbestätigungen.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b und lit. c DSGVO.

Empfänger: Twilio SendGrid Inc. (USA).

Speicherdauer: Versand- und Bounce-Protokolle beim Dienstleister bis zu neunzig Tage; der zugrunde liegende Kontobezug in unserer Datenbank richtet sich nach § 4.1. Zum Verhältnis zwischen Kontolöschung und den beim Dienstleister anfallenden technischen Versandprotokollen siehe § 9.2.

4.8 Newsletter (optional, mit Double-Opt-In)

Daten: E-Mail-Adresse, Double-Opt-In-Bestätigung, Versand-Status.

Zweck: Information über Produkt-Updates und Lerninhalte.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung), § 7 Abs. 2 Nr. 3 UWG.

Empfänger: Twilio SendGrid Inc. (USA) — derselbe Dienstleister wie für transaktionale E-Mails (§ 4.7).

Speicherdauer: bis zum Widerruf der Einwilligung; jede Newsletter-E-Mail enthält einen Abmeldelink. Der Nachweis der Einwilligung (Double-Opt-In-Protokoll) wird nach Widerruf bis zu drei Jahre als Beweissicherung aufbewahrt. Zum Verhältnis zur Kontolöschung siehe § 9.2.

4.9 Fehler-Tracking (Sentry) — nur mit Einwilligung

Daten: Browser-Stack-Traces, Geräte-Informationen, gekürzte IP-Adresse, gegebenenfalls Session-Replay (PII-gefiltert).

Zweck: Stabilitätsanalyse und Fehlerbehebung.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO sowie § 25 Abs. 1 TDDDG (Endgeräte-Einwilligung).

Empfänger: Functional Software, Inc. (USA).

Speicherdauer: Fehler-Events bis zu neunzig Tage.

Sentry wird ausschließlich nach ausdrücklicher Einwilligung im Cookie-Banner aktiviert. Ohne Einwilligung läuft die Plattform ohne Fehler-Tracking.

4.10 Reichweiten-Messung

ExamLab setzt derzeit **keinen separaten Webanalyse- oder Reichweiten-Messdienst** ein. Ein Tracking über einen Drittanbieter zu Reichweiten-Zwecken findet nicht statt. Sollte künftig ein solcher Dienst eingesetzt werden, erfolgt dies nur nach vorheriger Einwilligung, und diese Erklärung wird entsprechend aktualisiert.

4.11 Sicherheits- und Audit-Logs

Daten: Admin- und Nutzer-Aktionen, IP-Adresse (gekürzt erfasst, nach dreißig Tagen vollständig anonymisiert).

Zweck: IT-Sicherheit, Missbrauchsabwehr, forensische Aufklärung.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO i.V.m. Art. 32 DSGVO.

Speicherdauer: neunzig Tage; sicherheitsrelevante Ereignisse länger, soweit zur Aufklärung erforderlich.

4.12 Bearbeitung von DSGVO-Anfragen

Daten: Anfrage-Inhalt, Bearbeitungs-Status.

Zweck: Erfüllung der Pflichten aus Art. 12 ff. DSGVO.

Rechtsgrundlage: Art. 6 Abs. 1 lit. c DSGVO.

Speicherdauer: drei Jahre (Regelverjährungsfrist, §§ 195, 199 BGB).

4.13 Ground-Truth- und Kalibrierungsklausuren (Art. 14 DSGVO)

Daten: Texte echter, bereits benoteter Klausuren nebst zugehöriger Note, die zur Eichung und Qualitätssicherung der KI-Notenschätzung verwendet werden.

Zweck: Kalibrierung des Korrektur-Modells anhand realer Bewertungspaare (Text → Note), um die geschätzte Note belastbarer zu machen.

Datenschutzrechtliche Rechtsgrundlage: Vorrangig verarbeiten wir diese Klausuren **anonymisiert**; nach erfolgreicher Anonymisierung handelt es sich nicht mehr um personenbezogene Daten, sodass die DSGVO insoweit nicht anwendbar ist. Soweit vor oder während der Anonymisierung noch ein Personenbezug besteht, stützen wir die Verarbeitung auf **Art. 6 Abs. 1 lit. f DSGVO** (berechtigtes Interesse an einer verlässlichen, fairen Notenschätzung; die Interessenabwägung haben wir dokumentiert und stellen sie auf Anfrage bereit). Eine darauf bezogene urheberrechtliche Befugnis zur Auswertung der Texte (Text- und Data-Mining nach § 44b UrhG) betrifft allein das Urheberrecht und ist **keine** datenschutzrechtliche Rechtsgrundlage; sie tritt rein urheberrechtlich neben die vorstehende DSGVO-Grundlage, ohne sie zu ersetzen.

Besondere Kategorien: Sollten in den überlassenen Klausuren ausnahmsweise besondere Kategorien nach Art. 9 DSGVO enthalten sein, verarbeiten wir diese nur nach vorheriger Schwärzung/Anonymisierung oder, soweit ausnahmsweise erforderlich, auf Grundlage einer ausdrücklichen Einwilligung der betroffenen Person nach Art. 9 Abs. 2 lit. a DSGVO. Auf Art. 9 Abs. 2 lit. e DSGVO („offensichtlich öffentlich gemacht“) stützen wir uns dabei nicht, da von Korrektoren oder Studierenden überlassene Klausuren gerade nicht öffentlich gemacht wurden.

Quelle der Daten (Art. 14 Abs. 2 lit. f DSGVO): Die Klausuren stammen nicht von dir, sondern werden uns von Korrektoren bzw. Studierenden zur Verfügung gestellt. Klarnamen und sonstige Identifikatoren werden vor der Verarbeitung pseudonymisiert oder geschwärzt und sodann nach Möglichkeit anonymisiert.

Speicherdauer: so lange wie für die Kalibrierung erforderlich, längstens bis zum Wegfall des Eichzwecks.

Eine individuelle Benachrichtigung der ursprünglichen Verfasser unterbleibt, soweit sie sich nach Pseudonymisierung bzw. Anonymisierung als unmöglich oder unverhältnismäßig aufwendig erweist (Art. 14 Abs. 5 lit. b DSGVO). Auf Anfrage erteilen wir Auskunft, soweit eine Zuordnung noch möglich ist.

RECHTSDOKUMENT

§ 5 Cookies und vergleichbare Technologien

- 5.1** Beim ersten Besuch der Plattform wird ein Cookie-Banner eingeblendet, das eine granulare Auswahl ermöglicht und auf der ersten Ebene gleichrangig „Alle ablehnen“ und „Alle akzeptieren“ anbietet:
- **Technisch notwendig** (z. B. Session, CSRF-Token): werden ohne Einwilligung gesetzt; Rechtsgrundlage § 25 Abs. 2 Nr. 2 TDDDG.
 - **Funktional** (z. B. Theme-Präferenz, Schriftgröße): nur mit Einwilligung (§ 25 Abs. 1 TDDDG).
 - **Analyse** (z. B. Sentry-Performance und -Replay): nur mit Einwilligung (§ 25 Abs. 1 TDDDG).
 - **Marketing**: derzeit nicht im Einsatz.
- 5.2** Die Einwilligung kann jederzeit über den Link „Cookie-Einstellungen“ im Footer mit Wirkung für die Zukunft geändert oder widerrufen werden.

RECHTSDOKUMENT

§ 6 Rechte der betroffenen Person

Du hast jederzeit folgende Rechte:

- **Auskunft** über die zu deiner Person gespeicherten Daten (Art. 15 DSGVO).
- **Berichtigung** unrichtiger Daten (Art. 16 DSGVO).
- **Löschung** („Recht auf Vergessenwerden“, Art. 17 DSGVO).
- **Einschränkung** der Verarbeitung (Art. 18 DSGVO).
- **Datenübertragbarkeit** (Art. 20 DSGVO) — über die Funktion „Daten exportieren“ in den Einstellungen.
- **Widerspruch** gegen Verarbeitungen auf Grundlage berechtigter Interessen (Art. 21 DSGVO), insbesondere gegen die Verwendung als Kalibrierungsklausur (§ 4.13).
- **Widerruf** jeglicher Einwilligungen mit Wirkung für die Zukunft (Art. 7 Abs. 3 DSGVO), ohne dass die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung berührt wird.
- **Recht auf Eingreifen einer natürlichen Person, Standpunktdarlegung und Anfechtung** im Zusammenhang mit der automatisierten KI-Bewertung (Art. 22 Abs. 3 DSGVO), siehe § 4.4.
- **Information über die Datenquelle** bei nicht bei dir erhobenen Daten (Art. 14 Abs. 2 lit. f DSGVO), siehe § 4.2 und § 4.13.

Beschwerderecht (Art. 77 DSGVO): Du kannst dich unbeschadet anderer Rechtsbehelfe bei jeder Datenschutz-Aufsichtsbehörde beschweren, insbesondere bei der Behörde an deinem gewöhnlichen Aufenthaltsort, an deinem Arbeitsplatz oder am Ort des mutmaßlichen Verstoßes (Wahlrecht nach Art. 77 Abs. 1 DSGVO). Für den Verantwortlichen ist die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW), Kavalleriestraße 2–4, 40213 Düsseldorf, zuständig.

Anfragen richtest du bitte an datenschutz@exam-lab.de. Wir antworten unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags (Art. 12 Abs. 3 DSGVO). Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies wegen der Komplexität oder der Zahl der Anträge erforderlich ist; über eine solche Verlängerung samt Gründen unterrichten wir dich innerhalb eines Monats.

RECHTSDOKUMENT

§ 7 Drittländ-Übermittlungen

7.1 Hosting (Vercel, Railway, USA)

Einsatz: Frontend-Hosting (Vercel Inc., USA) und Backend-Hosting (Railway Corp., USA). Hierbei handelt es sich um einen eigenständigen Drittländtransfer, weil Konto-, Nutzungs- und ggf. Eingabedaten auf Servern in den USA verarbeitet werden.

Transfermechanismus: EU-US Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795 vom 10.07.2023) für nach dem DPF zertifizierte Empfänger; ergänzend bzw. als Fallback Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914) nebst zusätzlichen Schutzmaßnahmen (u. a. Transport- und Ruheverschlüsselung).

Hinweis: Da das Backend in den USA betrieben wird, können Kontodaten dort verarbeitet werden. Eine Verlegung des Backends in die Europäische Union ist geplant.

7.2 Anthropic PBC (USA)

Einsatz: Klausur-Korrektur, SLT-Feedback, KI-Tutor.

Transfermechanismus: EU-US Data Privacy Framework und Standardvertragsklauseln.

Speicherdauer beim Anbieter: bis zu dreißig Tage zur Missbrauchserkennung; kein Training auf Nutzerdaten (vertraglich vereinbart).

7.3 OpenAI L.L.C. (USA)

Einsatz: Transkription, ergänzende Korrekturen, Klassifikation.

Transfermechanismus: EU-US Data Privacy Framework und Standardvertragsklauseln.

Speicherdauer beim Anbieter: dreißig Tage; kein Training auf API-Daten (Standardeinstellung).

7.4 Mistral AI SAS (Frankreich, EU)

Einsatz: schnelle Klassifikationen, Routing-Layer.

Einordnung: Anbieter mit Sitz in der EU (Frankreich); es liegt **keine Drittländ-Übermittlung** vor. Mistral ist Auftragsverarbeiter; es besteht ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO, kein Training auf API-Daten. Die für die Verarbeitung maßgebliche Rechtsgrundlage des Verantwortlichen ist – wie bei den übrigen KI-Funktionen – Art. 6 Abs. 1 lit. b DSGVO (§ 4.4); ein gesonderter Transfermechanismus ist mangels Drittländbezug nicht erforderlich.

7.5 DeepSeek (Hangzhou) Technology Co., Ltd. (China)

Einsatz: eng begrenzte, gelegentliche Einzelaufgaben (z. B. punktuelle Karteikarten-Verfeinerung). Ein systematischer oder regelmäßiger Produktiveinsatz findet nicht statt.

Transfermechanismus: **Kein Angemessenheitsbeschluss.** Eine Übermittlung erfolgt nur als nicht-systematischer Einzelfall und nur, wenn du zuvor die **gesonderte, ausdrückliche Opt-in-Einwilligung** (separate Checkbox) nach Art. 49 Abs. 1 lit. a DSGVO erteilst; sie ist nicht im allgemeinen KI-Consent enthalten. Ohne diese Einwilligung wird DeepSeek nicht genutzt. In der Produktivumgebung sind China-Anbieter derzeit deaktiviert. Die Einwilligung ist jederzeit in den Einstellungen widerrufbar.

7.6 Moonshot AI / Kimi (China)

Einsatz: gelegentliche Long-Context-Verarbeitung als Einzelfall; kein systematischer Produktiveinsatz.

Transfermechanismus: wie § 7.5 — gesonderte Opt-in-Einwilligung nach Art. 49 Abs. 1 lit. a DSGVO erforderlich; ohne diese Einwilligung keine Übermittlung; in der Produktivumgebung derzeit deaktiviert.

7.7 Hinweis zu Risiken und Beschränkungen der China-Übermittlung

Für China besteht kein Angemessenheitsbeschluss. Das chinesische Recht (insbesondere PIPL, Data Security Law, Cybersecurity Law sowie das National Intelligence Law) begründet weitreichende behördliche Zugriffsmöglichkeiten ohne effektiven Rechtsschutz aus Sicht der betroffenen Person. Art. 49 Abs. 1 lit. a DSGVO trägt nur **gelegentliche, nicht-systematische** Übermittlungen. Wir setzen China-Anbieter deshalb ausschließlich für vereinzelte, nicht wiederkehrende Einzelfälle und nur nach deiner ausdrücklichen, gesonderten Einwilligung ein; im Produktivbetrieb sind sie deaktiviert. Ein regelmäßiger oder systematischer Einsatz, der über die Gelegentlichkeit hinausginge und Art. 49 als Grundlage ausschliesse, findet nicht statt; sollte ein solcher künftig vorgesehen werden, würden wir zuvor einen tauglichen Transfermechanismus schaffen und diese Erklärung aktualisieren.

7.8 Hinweis zu Modellen

Die jeweils eingesetzten Modelle der genannten Anbieter werden laufend an Stand der Technik, Verfügbarkeit und Leistungsfähigkeit angepasst. Die Liste der Anbieter selbst aktualisieren wir bei Änderungen unverzüglich in diesem Dokument.

7.9 Widerrufsmöglichkeit

Du kannst die Einwilligung in die Nutzung chinesischer Anbieter jederzeit in den Einstellungen widerrufen. In diesem Fall verwenden wir ausschließlich EU- oder DPF-konforme Anbieter; einzelne Funktionen können dadurch eingeschränkt sein.

RECHTSDOKUMENT

§ 8 Empfänger, Auftragsverarbeiter und sonstige Empfänger

Mit allen Auftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO. Google und Apple sind im Rahmen des Social-Logins **keine** Auftragsverarbeiter, sondern eigene Verantwortliche (§ 4.2); sie sind nachstehend gesondert als „eigene Verantwortliche“ gekennzeichnet.

Empfänger	Rolle	Zweck	Sitz / Transfermechanismus
Stripe Payments Europe Ltd. + Stripe Inc.	Auftragsverarbeiter	Zahlungsabwicklung	Irland / USA (DPF (EU) 2023/1795 + SCC)
Twilio SendGrid Inc.	Auftragsverarbeiter	transaktionale E-Mails + Newsletter-Versand	USA (DPF + SCC)
Functional Software, Inc. (Sentry)	Auftragsverarbeiter	Fehler-Tracking (nur mit Consent)	USA (DPF + SCC)
Anthropic PBC	Auftragsverarbeiter	KI-Korrektur, KI-Tutor	USA (DPF + SCC)
OpenAI L.L.C.	Auftragsverarbeiter	KI-Transkription, KI-Klassifikation	USA (DPF + SCC)
Mistral AI SAS	Auftragsverarbeiter	KI-Klassifikation	EU (Frankreich) — kein Drittland
Vercel Inc.	Auftragsverarbeiter	Frontend-Hosting	USA (DPF + SCC)
Railway Corp.	Auftragsverarbeiter	Backend-Hosting	USA (DPF + SCC) — Verlegung in die EU geplant
Google Ireland Ltd.	eigener Verantwortlicher	Social-Login	EU
Apple Distribution International Ltd.	eigener Verantwortlicher	Social-Login	EU
DeepSeek (Hangzhou) Technology Co., Ltd.	Empfänger im Drittland	KI-Modell	China — kein Angemessenheitsbeschluss; nur gelegentlich bei Opt-in (Art. 49 Abs. 1 lit. a); in Prod deaktiviert
Moonshot AI / Kimi	Empfänger im Drittland	KI Long-Context	China — kein Angemessenheitsbeschluss; nur gelegentlich bei Opt-in (Art. 49 Abs. 1 lit. a); in Prod deaktiviert

RECHTSDOKUMENT

§ 9 Löschung und Aufbewahrungsfristen

- 9.1

Personenbezogene Daten werden gelöscht oder anonymisiert, sobald der Zweck der Verarbeitung entfallen ist und keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- 9.2

Im Falle einer Accountlöschung gilt ein **30-Tage-Soft-Delete**, nach dessen Ablauf alle personenbezogenen Daten in unseren produktiven Systemen irreversibel gelöscht werden. Im Zuge der Löschung wird auch der verknüpfte Kundendatensatz beim Zahlungsdienstleister Stripe gelöscht, soweit keine handels- oder steuerrechtliche Aufbewahrungspflicht entgegensteht (§ 9.3). Nach der Kontolöschung übermitteln wir an Versanddienstleister (SendGrid) und Fehler-Tracking (Sentry) **keine neuen** personenbezogenen Daten mehr; bereits zuvor angefallene technische Protokolle dieser Auftragsverarbeiter (z. B. Versand- und Bounce-Protokolle, Fehler-Events) laufen jedoch nach deren jeweils eigenen, in § 4.7, § 4.8 und § 4.9 genannten kurzen Fristen (in der Regel bis zu neunzig Tage) automatisch aus; der Einwilligungsnachweis zum Newsletter wird als Beweissicherung bis zu drei Jahre vorgehalten. Ein Fortbestehen dieser technischen Protokolle widerspricht der Kontolöschung nicht, da insoweit kein neuer aktiver Datenfluss erfolgt.
- 9.3

Gesetzliche und vertragliche Aufbewahrungsfristen:

- Rechnungs- und Buchhaltungsdaten: zehn Jahre (§ 257 HGB, § 147 AO).
- Steuerlich relevante Vertragsunterlagen: zehn Jahre (§ 147 AO).
- Einwilligungsnachweise: drei Jahre (Beweissicherung).
- DSGVO-Anfragen: drei Jahre (§ 4.12).
- Versand- und Bounce-Protokolle (SendGrid): bis zu neunzig Tage (§ 4.7, § 4.8).
- Fehler-Events (Sentry): bis zu neunzig Tage (§ 4.9).
- Sicherheits- und Audit-Logs: neunzig Tage, IP nach dreißig Tagen anonymisiert (§ 4.11).

RECHTSDOKUMENT

§ 10 Technische und organisatorische Maßnahmen (TOMs)

Wir setzen Maßnahmen nach Art. 32 DSGVO ein, insbesondere:

- Transportverschlüsselung (TLS 1.2 oder höher) und HSTS.
- Passwort-Hashing mit bcrypt (13 Runden); Zwei-Faktor-Authentifizierung per TOTP optional.
- CSRF-Schutz (Double-Submit), Rate-Limits, Brute-Force-Schutz.
- PII-Filter (Pseudonymisierung direkter Identifikatoren) vor externen API-Aufrufen, insbesondere an KI-Anbieter; ergänzend Hinweise zur Datenminimierung an den Eingabefeldern, da der Filter besondere Kategorien nach Art. 9/10 DSGVO nicht erkennt (§ 4.4).
- IP-Kürzung und nachgelagerte Anonymisierung in Logs.
- Strikte Zugriffskontrolle; keine produktiven Daten auf Entwickler-Geräten.
- Tägliche Backups mit verschlüsselter Offsite-Ablage.
- Cookie-Banner mit granularer Einwilligung und gleichrangiger Ablehnungsoption.
- Sentry-Initialisierung nur nach Einwilligung.

RECHTSDOKUMENT

§ 11 Datenschutz-Folgenabschätzung (DSFA)

- 11.1** Aufgrund der KI-gestützten Verarbeitung von Lerndaten und der Möglichkeit, dass Klausurtexte besondere Kategorien nach Art. 9 DSGVO berühren können (z. B. Sachverhalte im Sozial-, Familien- oder Strafrecht), führen wir für die betroffenen Verarbeitungen eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durch. Die DSFA wird vor Aufnahme einer neuen risikobehafteten Verarbeitung durchgeführt und bei wesentlichen Änderungen überprüft und fortgeschrieben.
- 11.2** Die DSFA wird intern dokumentiert. Aufsichtsbehörden sowie betroffene Personen mit berechtigtem Interesse erhalten auf schriftliche Anfrage an `datenschutz@exam-lab.de` Auskunft über die Ergebnisse, soweit Geschäfts- oder Betriebsgeheimnisse nicht entgegenstehen.

RECHTSDOKUMENT

§ 12 Ablauf der Übermittlung an KI-Anbieter

Bei jeder Übermittlung an einen KI-Anbieter werden folgende Schritte durchgeführt:

1. Die Eingabe durchläuft den PII-Filter (§ 4.4), der direkte Identifikatoren entfernt oder pseudonymisiert (besondere Kategorien nach Art. 9/10 DSGVO werden hierbei nicht zuverlässig erkannt; siehe Hinweis in § 4.4).
2. Der gefilterte Text wird über eine verschlüsselte HTTPS-Verbindung an den KI-Anbieter übermittelt.
3. Die KI-Ausgabe wird empfangen, in der Datenbank gespeichert und dem Nutzer als „KI-generiert“ markiert dargestellt (Art. 50 KI-VO).
4. Beim erstmaligen Aufruf einer Funktion, die ausnahmsweise einen chinesischen Anbieter erfordert, wird die gesonderte, ausdrückliche Einwilligung des Nutzers für diese nur gelegentliche Drittlandübermittlung eingeholt (Art. 49 Abs. 1 lit. a DSGVO).

RECHTSDOKUMENT

§ 13 Änderungen dieser Datenschutzerklärung

Wir aktualisieren diese Erklärung, wenn sich Verarbeitungen, Anbieter oder die Rechtslage ändern. Die jeweils aktuelle Fassung ist auf exam-lab.de abrufbar. Wesentliche Änderungen kündigen wir im Voraus per E-Mail an.