

Vertrag über die Auftragsverarbeitung (AVV)

nach Art. 28 DSGVO für das Nachweisportal „Lexjo“

Fassung 1.0 · Stand 01.11.2026

Verantwortlicher: das Unternehmen, das im Portal eine entgeltliche Nutzung gebucht hat (nachfolgend „Kunde“).

Auftragsverarbeiter: Christian Scur, Schulstr. 7, 15344 Strausberg, info@lexjo.de (nachfolgend „Betreiber“).

Dieser Vertrag wird bei der Buchung im Portal geschlossen (Art. 28 Abs. 9 DSGVO). Das Portal hält Fassung, Zeitpunkt und erklärende Person fest; der Kunde kann den Vertrag jederzeit auf der Vertragsseite abrufen.

§ 1 Gegenstand und Dauer

(1) Der Betreiber stellt dem Kunden das Nachweisportal Lexjo nach seinen Allgemeinen Geschäftsbedingungen (AGB) bereit und verarbeitet dabei personenbezogene Daten im Auftrag des Kunden. Dieser Vertrag regelt die datenschutzrechtlichen Pflichten dazu. In Fragen des Datenschutzes geht er den AGB vor.

(2) Der Vertrag gilt, solange der Betreiber Daten im Auftrag des Kunden verarbeitet: für die Laufzeit der entgeltlichen Nutzung, den anschließenden Nachlauf (§ 17 Abs. 2 AGB) und bis zum Abschluss der Löschung (§ 8).

§ 2 Zweck, Art und Umfang der Verarbeitung

(1) Zweck ist das Anfordern, Prüfen, Klären, Überwachen und Dokumentieren der Nachweise der Dienstleister und Nachunternehmer des Kunden einschließlich der automatischen Plausibilitätsprüfung (§ 2 Abs. 4 AGB) sowie die Aufbewahrung der Akten als Beleg der Prüfung.

(2) Art der Verarbeitung: Speichern, Ordnen, Anzeigen, automatisches Auswerten, Übermitteln per E-Mail, Exportieren, Archivieren und Löschen.

(3) Datenarten: Stammdaten und Ansprechpartner der Dienstleister und Lieferanten des Kunden; Nachweisdokumente mit den darin enthaltenen Angaben, etwa Namen, Geburtsdaten und Anschriften von Inhabern und Geschäftsführern in Register- und Gewerbeunterlagen, Steuer- und Betriebsnummern sowie Angaben aus Bescheinigungen von Behörden, Krankenkassen, Berufsgenossenschaften und Versicherern; Prüfentscheidungen, Nachrichten, Notizen und die Chronik der Akte mit den Namen der handelnden Personen; Benachrichtigungen und E-Mails.

(4) Betroffene Personen: Zugangsinhaber und Beschäftigte des Kunden; Inhaber, Geschäftsführer, Vertretungsberechtigte, Ansprechpartner und Beschäftigte der Dienstleister; in Nachweisen genannte Bedienstete der ausstellenden Stellen sowie sonstige Dritte, die auf den hochgeladenen Dokumenten erkennbar sind.

(5) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden nicht verarbeitet. Auszüge aus dem Gewerbezentralregister können Angaben im Sinne des Art. 10 DSGVO enthalten; der Kunde stellt sicher, dass er sie verlangen darf.

(6) Nicht Gegenstand dieses Vertrags sind die Benutzerkonten, die Vertrags- und Abrechnungsdaten und die technischen Betriebsdaten; dafür ist der Betreiber selbst Verantwortlicher, und es gilt seine Datenschutzerklärung. Für die Angaben, die ein Dienstleister selbst über sein Unternehmen einstellt, ist dieser verantwortlich.

§ 3 Weisungen

(1) Der Betreiber verarbeitet die Daten nur auf dokumentierte Weisung des Kunden. Weisungen sind dieser Vertrag, die AGB und jede Nutzung der Portalfunktionen durch Zugänge des Kunden, zum Beispiel Einladen, Festlegen von Anforderungen, Freigeben und Ablehnen, Beenden einer Zusammenarbeit, Einstellen der Aufbewahrungsdauer und Export. Dazu gehört auch die Aufbewahrung von Fassungen im Sperrarchiv nach § 11 Abs. 8 und 9 AGB, auch wenn der Dienstleister widerspricht.

(2) Einzelweisungen erteilen Admin-Zugänge des Kunden in Textform an info@lexjo.de.

(3) Hält der Betreiber eine Weisung für datenschutzwidrig, weist er den Kunden unverzüglich darauf hin und darf die Ausführung bis zur Klärung aussetzen.

(4) Eine Übermittlung in ein Land außerhalb der EU und des EWR erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO. Die betroffenen Unterauftragsverarbeiter und die jeweilige Grundlage nennt Anlage 2.

§ 4 Vertraulichkeit

Zugang zu den Daten erhalten nur Personen, die zur Vertraulichkeit verpflichtet sind, und nur soweit es für die Leistung erforderlich ist. Die Pflicht gilt über das Ende dieses Vertrags hinaus.

§ 5 Sicherheit der Verarbeitung

Der Betreiber trifft die technischen und organisatorischen Maßnahmen nach Anlage 1 und hält sie aufrecht. Er darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf dabei nicht sinken.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter. Der Betreiber verpflichtet jeden von ihnen vertraglich auf die Pflichten dieses Vertrags (Art. 28 Abs. 4 DSGVO) und haftet für ihn wie für eigenes Handeln.

(2) Einen neuen oder ersetzten Unterauftragsverarbeiter kündigt der Betreiber mindestens zwei Wochen vor dem Einsatz per E-Mail an die Admin-Zugänge des Kunden an, mit Name, Sitz, Leistung, Datenarten und Ort der Verarbeitung. Der Kunde kann binnen zwei Wochen nach Zugang aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Kann der Betreiber den Unterauftragsverarbeiter dann für den Kunden nicht ausschließen, kann jede Partei den Vertrag über die Nutzung des Portals zum Zeitpunkt des Einsatzes kündigen. Ohne Widerspruch gilt der Einsatz als genehmigt. Die E-Mail, mit der er über den neuen Unterauftragsverarbeiter informiert wird, weist ihn auf die Folgen eines fehlenden Widerspruchs hin.

(3) Die Unterauftragsverarbeiter nach Anlage 2 setzen ihrerseits weitere Unterauftragsverarbeiter ein. Der Betreiber verpflichtet sie, dabei die Anforderungen des Art. 28 Abs. 4 DSGVO einzuhalten. Über Änderungen auf dieser Ebene informiert der Betreiber den Kunden unverzüglich, nachdem er selbst davon erfahren hat; Absatz 2 Satz 3 bis 5 gilt entsprechend, die Frist für den Widerspruch beginnt mit dieser Information.

§ 7 Unterstützung des Kunden

(1) Anfragen betroffener Personen erfüllt der Kunde in erster Linie selbst über die Funktionen des Portals (Einsicht, Export der Akte, Berichtigung, Beenden der Zusammenarbeit). Anfragen, die beim Betreiber eingehen, leitet dieser unverzüglich an den Kunden weiter. Muss eine Nachweisdatei entfernt werden, entfernt der Betreiber sie auf Weisung und vermerkt dies in der Chronik der betroffenen Akten.

(2) Eine Verletzung des Schutzes personenbezogener Daten, die Daten des Kunden betrifft, meldet der Betreiber unverzüglich, spätestens 48 Stunden nach Kenntnis, per E-Mail an die Admin-Zugänge des Kunden, soweit bekannt mit den Angaben nach Art. 33 Abs. 3 DSGVO. Er unterstützt den Kunden bei der Meldung an die Aufsichtsbehörde und der Benachrichtigung der Betroffenen.

(3) Bei einer Datenschutz-Folgenabschätzung und einer Konsultation der Aufsichtsbehörde unterstützt der Betreiber den Kunden mit den ihm vorliegenden Informationen.

(4) Unterstützung, die über die Funktionen des Portals hinausgeht und nicht auf einem Verstoß des Betreibers beruht, kann der Betreiber nach vorheriger Ankündigung nach Aufwand berechnen.

§ 8 Löschung und Rückgabe

(1) Während der Laufzeit löscht der Betreiber Daten automatisch nach den Fristen der AGB. Akten beendeter Zusammenarbeiten und archivierte Fassungen von Nachweisen werden drei Jahre ab dem 1. Januar des auf die Beendigung bzw. den Rückzug folgenden Jahres aufbewahrt; der Kunde kann diese Dauer auf höchstens 30 Jahre verlängern, aber nicht verkürzen (§ 11 Abs. 8 und 9 AGB). Danach werden sie gelöscht.

(2) Nach dem Vertragsende kann der Kunde seine Akten während des Nachlaufs ansehen und herunterladen (§ 17 Abs. 2 AGB); das ist die Rückgabe der Daten. Danach löscht der Betreiber alle im Auftrag des Kunden verarbeiteten Daten (§ 17 Abs. 3 AGB). Die Nachweise der Dienstleister bleiben in deren Unternehmen (§ 17 Abs. 4 AGB).

(3) Ausgenommen sind Daten, die der Betreiber aufgrund gesetzlicher Pflichten aufbewahren muss, und Sicherungskopien zum Zwecke der (System-)Wiederherstellung (sog. Back-ups) bis zu ihrer turnusmäßigen Löschung (Anlage 1 Nr. 4). Auf Verlangen bestätigt der Betreiber die Löschung in Textform.

§ 9 Nachweise und Kontrollen

(1) Der Betreiber stellt dem Kunden auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlich sind, insbesondere die Anlagen dieses Vertrags und die Nachweise seiner Unterauftragsverarbeiter.

(2) Darüber hinaus kann der Kunde die Einhaltung dieses Vertrags einmal im Kalenderjahr und bei konkretem Anlass selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer kontrollieren, nach Ankündigung mit angemessener Frist, in der Regel vier Wochen, und vorrangig durch Einsicht in Unterlagen. Eigene Rechenzentren unterhält der Betreiber nicht; für diese gelten die Nachweise der Anbieter.

§ 10 Zugriffe des Betreibers im Einzelfall

Auf Nachweise und Akten des Kunden greift der Betreiber nur zu, um ein Löschverlangen, die Entfernung eines unzulässigen Inhalts, eine behördliche oder gerichtliche Anordnung, eine gesetzliche Pflicht oder eine Weisung des Kunden umzusetzen sowie zur stichprobenweisen Qualitätssicherung der automatischen Prüfung (§ 2 Abs. 4 AGB). Jede Entfernung wird unveränderbar protokolliert. Der Betreiber bewertet keine Nachweise und bearbeitet keine Akten des Kunden.

§ 11 Schlussbestimmungen

(1) Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln der AGB.

(2) Neue Fassungen dieses Vertrags stellt der Betreiber wie neue Fassungen der AGB bereit; § 16 AGB gilt entsprechend.

(3) Im Übrigen gilt § 18 AGB.

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Betreiber ist Einzelunternehmer und betreibt keine eigenen Server. Die Verarbeitung findet bei den Unterauftragsverarbeitern nach Anlage 2 statt. Die folgenden Maßnahmen gelten für die Daten, die der Betreiber im Auftrag des Kunden verarbeitet.

1. Zutritt und Infrastruktur

- Datenbank, Dateispeicher und Anwendung laufen in Rechenzentren in der EU (Frankfurt am Main), deren Betreiber nach ISO/IEC 27001 und SOC 2 zertifiziert sind; Zutrittskontrolle und Überwachung leisten diese Anbieter.
- Auf den Arbeitsgeräten des Betreibers werden keine Daten des Kunden dauerhaft gespeichert; der Zugriff erfolgt über den Browser.

2. Zugang und Anmeldung

- Anmeldung mit E-Mail-Adresse und Passwort; Passwörter mit mindestens 10 Zeichen aus Groß- und Kleinbuchstaben, Ziffer und Sonderzeichen; gespeichert wird nur ein Hash.
- Einladungslinks enthalten einen Zufallswert, gelten 14 Tage, sind nur einmal verwendbar und nur mit der eingeladenen E-Mail-Adresse annehmbar.
- Der Betreiber-Bereich ist nur für hinterlegte Adressen erreichbar und verlangt einen zweiten Anmeldefaktor (TOTP), der nach zwei Stunden erneut abgefragt wird.
- Zugangsschlüssel zu Datenbank und Diensten liegen nur auf dem Server, nie im Browser oder im Quellcode. Die Konten bei den Anbietern sind mit einem zweiten Faktor geschützt.

3. Zugriff und Trennung

- Zugriffsregeln in der Datenbank (Row-Level Security) auf jeder Tabelle nach dem Grundsatz: verboten ist, was nicht ausdrücklich erlaubt ist.
- Nachweise sieht nur der Dienstleister selbst und ein Auftraggeber mit aktiver Verknüpfung; jeder Auftraggeber hat eigene Prüfentscheidungen, Notizen und ein eigenes Sperrarchiv.
- Rollen im Unternehmen (Inhaber, Admin, Mitarbeiter); Änderungen nur über geprüfte Datenbankfunktionen.
- Dateien liegen in privaten Speichern und werden nur über signierte Links mit kurzer Laufzeit (zwei Minuten, im Betreiber-Bereich fünf Minuten) geöffnet.
- Der Betreiber findet Nachweise nur über Metadaten (Unternehmen, Zeitraum, Nachweisart); einen Volltextindex gibt es nicht. Weitere Betreiber-Zugänge können ohne Lösch- und Änderungsrechte eingerichtet werden.

4. Verschlüsselung, Sicherung und Verfügbarkeit

- Verschlüsselte Übertragung (TLS) auf allen Wegen; Verschlüsselung im Ruhezustand bei Datenbank, Dateispeicher und Sicherungen.
- Tägliche Sicherung der Datenbank durch den Anbieter; tägliche, versionierte Sicherung der Dateien in einem getrennten Speicher in Deutschland. Versionen gelöschter Dateien werden dort nach 30 Tagen entfernt.
- Der Kunde kann jede Akte jederzeit als ZIP-Datei herunterladen.

5. Nachvollziehbarkeit

- Jede Akte hat eine Chronik mit Zeitpunkt und handelnder Person, die technisch gegen Ändern und Löschen gesperrt ist; gelöscht wird sie nur nach Ablauf der Frist.

- Entfernungen von Dateien und Änderungen an Betreiber-Zugängen stehen in einem unveränderbaren Protokoll.
- Zustimmungen zu AGB und AVV werden mit Fassung, Person und Zeitpunkt festgehalten.

6. Datensparsamkeit und Löschung

- Ein automatischer Löschlauf löscht nach den vereinbarten Fristen; sein Protokoll enthält nur Zählwerte, keine Personendaten.
- E-Mails enthalten keine Freitexte aus Nachrichten und Notizen; das Portal setzt keine Tracking- oder Werbedienste ein.
- Inhalte werden nicht zum Training von Sprachmodellen verwendet. Für die automatische Prüfung erhält der Anbieter nur den einzelnen Nachweis und die zum Abgleich nötigen Angaben.

7. Organisation und regelmäßige Überprüfung

- Weitere Personen erhalten Zugang zu Daten des Kunden nur nach schriftlicher Verpflichtung auf Vertraulichkeit.
- Quellcode in einem privaten Repository; Änderungen an der Datenbank nur als geprüfte Migrationen mit automatisierten Tests; Sicherheitsüberprüfung bei größeren Änderungen.
- Verfahren bei Datenpannen: erkennen, bewerten, eindämmen (etwa Schlüssel austauschen, Zugang sperren), dem Kunden binnen 48 Stunden melden, dokumentieren.
- Jährliche Überprüfung dieser Maßnahmen und der Nachweise der Unterauftragsverarbeiter.

Anlage 2 — Unterauftragsverarbeiter (Stand 01.11.2026)

Der Kunde genehmigt den Einsatz der folgenden Unterauftragsverarbeiter (§ 6 Abs. 1). Änderungen kündigt der Betreiber nach § 6 Abs. 2 an.

Anbieter	Leistung	Ort der Verarbeitung	Grundlage
Supabase, Inc., USA	Datenbank, Dateispeicher und Anmeldung	EU (Frankfurt am Main), Rechenzentren von Amazon Web Services	Standardvertragsklauseln für mögliche Zugriffe aus den USA
Vercel Inc., USA	Betrieb der Anwendung (Hosting)	EU (Frankfurt am Main)	Standardvertragsklauseln für mögliche Zugriffe aus den USA
Scaleway SAS, Paris, Frankreich	Versand der E-Mails des Portals	Frankreich (Paris)	EU, keine Übermittlung in Drittländer
Amazon Web Services EMEA SARL, Luxemburg	Automatische Plausibilitätsprüfung über Amazon Bedrock (Sprachmodell Claude von Anthropic): Inhalt des Nachweises und die Angaben zum Abgleich	EU (Anfrage in Frankfurt am Main; Verarbeitung in Rechenzentren in Deutschland, Frankreich, Irland, Italien, Schweden und Spanien)	EU; Standardvertragsklauseln für mögliche Zugriffe aus den USA; keine Verwendung zum Training
Hetzner Online GmbH, Gunzenhausen, Deutschland	Verschlüsselte Sicherungskopie der Dateien	Deutschland	EU, keine Übermittlung in Drittländer
united-domains GmbH, Starnberg, Deutschland	E-Mail-Postfächer des Betreibers (etwa Weisungen und Anfragen an info@lexjo.de)	Deutschland	EU, keine Übermittlung in Drittländer