SICHERHEIT UND VERTRAUEN

Vertrauenspaket Lexploris

Neuralis GmbH i.G., Stephansplatz 8/20, 1010 Wien · Stand 24.10.2026 · Fragen an security@lexploris.com

Dieses Paket fasst zusammen, wie wir Daten schützen, wo sie verarbeitet werden und welche Dienstleister wir einsetzen. Es hilft Ihnen bei der Bewertung Ihrer Lieferanten, etwa nach § 32 Abs. 4 lit. d NISG 2026. Die jeweils aktuelle Fassung finden Sie unter https://www.lexploris.com/sicherheit.

Inhalt

1. Hosting- und Sicherungsnachweis
2. Antworten für Lieferanten-Fragebögen
3. Auftragsverarbeitungsvertrag (AVV)
4. Unterauftragnehmer

1. Hosting- und Sicherungsnachweis

Thema	Angabe
Standort	Gemieteter Server der netcup GmbH in einem Rechenzentrum in Wien, Österreich
Betrieb	Anwendung, Datenbank, Dateien und Sicherungen auf diesem Server; TLS endet auf dem Server, kein Dienstleister dazwischen
Sicherung	Täglich Datenbank, Dateien und Archiv; mit AES-256 verschlüsselt, bevor sie den Server verlassen
Aufbewahrung	14 Tage auf dem Server, höchstens 30 Tage als zweite Kopie
Zweiter Standort	Verschlüsselte Kopie auf einem eigenen Server des Betreibers in versperrten Räumlichkeiten in Österreich; Abholung über ein Konto, das nur Sicherungsdateien lesen kann
Wiederherstellungsziele	Höchstens 24 Stunden Datenverlust (RPO), Wiederherstellung binnen 4 Stunden (RTO)
Wiederherstellungstest	17.10.2026 mit der Live-Sicherung des damaligen Betriebs bestanden (Datenbank in 49 Sekunden wiederhergestellt, eine manipulierte Kopie wurde abgelehnt); 20.10.2026 Probelauf auf dem Server in Wien mit Demodaten bestanden; Wiederholung vierteljährlich, nächster Test Jänner 2027
Überwachung	Container-Wache alle 5 Minuten, Prüfung von außen alle 30 Minuten, tägliche Prüfung von Datenquellen, Speicherplatz und Alter der Sicherung; Alarm per E-Mail
Verfügbarkeit	Ziel 99,5 % im Monatsmittel, ohne Gewähr; feste Servicelevels nur im Angebot für Enterprise
KI	Sprachmodelle von Mistral AI in der Europäischen Union, kein Training mit den Daten; nur bei Störungen vorübergehend Amazon Bedrock in Frankfurt am Main

2. Antworten für Lieferanten-Fragebögen

Gegliedert nach den Inhalten des § 32 Abs. 4 NISG 2026. Angaben, die noch fehlen, sind als „Angabe folgt“ gekennzeichnet. Verbindlich sind der Auftragsverarbeitungsvertrag mit seinen Anlagen und Ihr Vertrag.

Unternehmen und Ansprechpersonen

Wer ist der Anbieter?
Neuralis GmbH i.G. (Gesellschaft mit beschränkter Haftung in Gründung), Stephansplatz 8/20, 1010 Wien, Österreich. Lexploris ist eine Marke der Neuralis GmbH i.G..

Wer vertritt das Unternehmen?
Die Geschäftsführung nennt das Impressum.

Firmenbuchnummer und UID-Nummer?
Angabe folgt. Bitte fragen Sie bei security@lexploris.com an.

An wen richten wir Fragen zur Sicherheit?
An security@lexploris.com. Schwachstellen melden Sie vertraulich an dieselbe Adresse (security.txt). Wir bestätigen den Eingang binnen 2 Werktagen und melden uns binnen 10 Werktagen mit einer Einschätzung.

Fällt Lexploris selbst unter das NISG 2026?
Nach unserer Einschätzung vom 16.10.2026 nein. Wir beantworten Fragen zur Sicherheit der Lieferkette trotzdem, damit Sie Ihre Pflichten nach § 32 Abs. 4 lit. d NISG 2026 erfüllen können.

Datenschutz und Standort

Wo werden unsere Daten verarbeitet?
Auf einem gemieteten Server von netcup in einem Rechenzentrum in Wien. Eine zweite, verschlüsselte Kopie der Sicherungen liegt auf einem eigenen Server des Betreibers in Österreich. Die Sprachmodelle laufen bei Mistral AI in der EU.

Gibt es einen Auftragsverarbeitungsvertrag?
Ja. Der AVV nach Art. 28 DSGVO ist Bestandteil jedes Vertrags und wird mit dem Hauptvertrag geschlossen. Auf Wunsch stellen wir eine unterschriebene Fassung bereit.

Werden Daten in Drittländer übermittelt?
Die Unterauftragsverarbeiter verarbeiten die Daten in der EU. Setzt Mistral AI eigene Dienstleister außerhalb der EU ein, gelten Standardvertragsklauseln. Amazon Web Services (nur Ausweich bei Störungen) verarbeitet in Frankfurt am Main, gehört aber zu einem Konzern mit Sitz in den USA; dafür gelten das EU-US Data Privacy Framework und ergänzend Standardvertragsklauseln.

Werden unsere Daten zum Training von KI verwendet?
Nein. Jede KI-Aussage braucht ein wörtliches, automatisch geprüftes Zitat aus der Quelle. Auf Verlangen in Textform schalten wir die KI-Bewertung für Ihre Organisation ab; Lexploris arbeitet dann regelbasiert weiter.

Wie schnell melden Sie eine Verletzung des Schutzes personenbezogener Daten?
Ohne unangemessene Verzögerung, spätestens 48 Stunden nach Kenntnis, an die in Lexploris hinterlegte Adresse der Administration.

Was passiert mit den Daten bei Vertragsende?
Sie können Ihre Daten jederzeit selbst exportieren, nach Vertragsende noch 30 Tage. Danach löschen wir sie. Sicherungskopien werden spätestens 30 Tage nach der Löschung überschrieben. Die Löschung bestätigen wir auf Anfrage in Textform.

Dürfen wir prüfen?
Ja. Sie oder ein zur Verschwiegenheit verpflichteter Prüfer dürfen nach 14 Tagen Vorankündigung prüfen, in der Regel einmal je Jahr, vorrangig durch Auskünfte und Unterlagen.

§ 32 Abs. 4 lit. a NISG 2026: Risikoanalyse und Sicherheit der Informationssysteme

Gibt es eine Risikoanalyse?
Ja. Ein Bedrohungsmodell deckt Anwendung, Betrieb, Schnittstellen, KI und Lieferkette ab (Fassung 0.3 vom 20.10.2026, in Prüfung). Restrisiken nimmt die Geschäftsführung schriftlich an oder lässt sie beheben. Eine Zusammenfassung erhalten Sie auf Anfrage.

Wie sind die Daten der Kunden voneinander getrennt?
Jede Abfrage ist auf die eigene Organisation beschränkt. Eine zweite Schutzebene bilden Zeilenrechte (Row Level Security) in PostgreSQL für alle mandantenbezogenen Tabellen.

§ 32 Abs. 4 lit. b NISG 2026: Bewältigung von Sicherheitsvorfällen

Gibt es einen Prozess für Sicherheitsvorfälle?
Ja. Vorfälle werden in vier Schweregrade eingestuft. Beim höchsten Grad (Dienst nicht erreichbar, Datenverlust, Verdacht auf Datenleck) beginnen wir sofort und informieren betroffene Kunden binnen 1 Stunde. Für Ausfall, Sicherung, Datenpanne und Auslieferung gibt es schriftliche Abläufe.

Wann reagieren Sie auf Alarme?
Montag bis Freitag von 8 bis 18 Uhr (Wien) binnen 1 Stunde. Außerhalb dieser Zeiten nach bestem Bemühen; Vorfälle des höchsten Grades möglichst am selben Tag.

Wie werden wir informiert?
Per E-Mail an die Administration Ihrer Organisation und über die Statusseite.

§ 32 Abs. 4 lit. c NISG 2026: Aufrechterhaltung des Betriebs, Sicherung und Wiederherstellung

Wie werden die Daten gesichert?
Täglich Datenbank, Dateien und Archiv, mit AES-256 verschlüsselt. Aufbewahrung 14 Tage auf dem Server und höchstens 30 Tage als zweite Kopie an einem getrennten Ort in Österreich.

Wird die Wiederherstellung getestet?
Ja, vierteljährlich und nach jeder Änderung an Sicherung oder Datenbank. Zuletzt am 17.10.2026 mit der Live-Sicherung (bestanden) und am 20.10.2026 auf dem Server in Wien mit Demodaten (bestanden).

Welche Wiederherstellungsziele gelten?
Höchstens 24 Stunden Datenverlust (RPO) und Wiederherstellung binnen 4 Stunden (RTO).

Kann eine fehlerhafte Version zurückgenommen werden?
Ja. Vor jeder Auslieferung wird gesichert. Die Rücknahme auf die vorige Version ist geübt (Probelauf 20.10.2026: 10 Sekunden).

Wer vertritt die verantwortliche Person bei Ausfall?
Angabe folgt. Bitte fragen Sie bei security@lexploris.com an.

§ 32 Abs. 4 lit. d NISG 2026: Sicherheit der Lieferkette

Welche Dienstleister verarbeiten unsere Daten?
netcup GmbH (Server in Wien), Mistral AI SAS (Sprachmodelle in der EU) und webgo GmbH (System-E-Mails, Deutschland). Amazon Web Services (Bedrock, Frankfurt am Main) nur als Ausweich bei Störungen der KI. Die vollständige Liste steht auf der Seite Unterauftragnehmer.

Wie sind die Dienstleister verpflichtet?
Jeder Unterauftragsverarbeiter ist vertraglich auf ein gleichwertiges Schutzniveau verpflichtet (Art. 28 Abs. 4 DSGVO). Wir haften für die Einhaltung.

Erfahren wir von neuen Dienstleistern?
Ja, mindestens 30 Tage vorher in Textform. Sie können aus datenschutzrechtlichen Gründen widersprechen.

Wie gehen Sie mit Software-Abhängigkeiten um?
Abhängigkeiten stehen in festen Versionen. Die CI prüft bei jeder Änderung auf bekannte Schwachstellen und prüft die Signaturen der Pakete. Für Release-Versionen erzeugt die CI eine Stückliste der Software (SBOM, CycloneDX).

§ 32 Abs. 4 lit. e NISG 2026: Entwicklung, Wartung und Umgang mit Schwachstellen

Wie wird die Software entwickelt und geprüft?
Jede Änderung läuft über einen Pull Request mit Code-Review, automatischen Tests (darunter Mandantentrennung und Berechtigungen), Suche nach Geheimnissen im Code und Prüfung der Abhängigkeiten.

Sind Entwicklung, Test und Betrieb getrennt?
Ja. Entwicklung und Testsystem laufen auf einem eigenen System, getrennt vom Betrieb und nur mit Demodaten. Automatische Tests nutzen eine getrennte Testdatenbank.

Wie werden Server aktuell gehalten?
Das Betriebssystem spielt Sicherheitsupdates automatisch ein. Die Anwendung wird als geprüfte Version mit Sicherung vorab ausgeliefert.

Gibt es einen Penetrationstest?
Noch nicht. Ein Test durch externe Prüfer ist geplant, danach in regelmäßigen Abständen.

§ 32 Abs. 4 lit. f NISG 2026: Bewertung der Wirksamkeit

Wie prüfen Sie, ob die Maßnahmen wirken?
Wir überprüfen die technischen und organisatorischen Maßnahmen mindestens jährlich und bei wesentlichen Änderungen. Verfügbarkeit und Aktualität der Datenquellen messen wir laufend gegen festgelegte Ziele. Vor dem Start mit zahlenden Kunden prüfen wir die Betriebsbereitschaft nach einer festen Liste.

Gibt es eine unabhängige Prüfung?
Noch nicht. Der geplante Penetrationstest ist der erste Schritt.

§ 32 Abs. 4 lit. g NISG 2026: Cyberhygiene und Schulungen

Welche Grundregeln gelten im Betrieb?
Anmeldung am Server nur mit Schlüssel, eingehend nur SSH und HTTPS, Schutz vor wiederholten Fehlversuchen, administrativer Zugang nur mit Zwei-Faktor-Anmeldung. Geheimnisse liegen nie im Code.

Werden die Beschäftigten zur Sicherheit geschult?
Angabe folgt. Bitte fragen Sie bei security@lexploris.com an.

§ 32 Abs. 4 lit. h NISG 2026: Kryptografie und Verschlüsselung

Wie werden Daten bei der Übertragung geschützt?
Ausschließlich über TLS mit HTTP Strict Transport Security. TLS endet auf unserem Server.

Wie werden gespeicherte Daten geschützt?
Sicherungen sind mit AES-256 verschlüsselt, bevor sie den Server verlassen; den Schlüssel hat nur der Betreiber. Passwörter sind mit Argon2id gehasht, API-Schlüssel nur als Hash gespeichert, Geheimnisse für Schnittstellen verschlüsselt. Webhooks sind mit HMAC signiert.

Sind die Datenträger des Servers verschlüsselt?
Angabe folgt. Bitte fragen Sie bei security@lexploris.com an.

§ 32 Abs. 4 lit. i NISG 2026: Personal, Zugriffskontrolle und Verwaltung der Anlagen

Wer hat administrativen Zugriff?
Nur namentlich benannte Personen, mit Zwei-Faktor-Anmeldung und persönlichen Schlüsseln. Derzeit ist das allein der Geschäftsführer.

Sind die Personen zur Vertraulichkeit verpflichtet?
Ja. Wir setzen nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (§ 6 DSG), auch nach Ende der Tätigkeit.

Wie steuern Sie Rechte in der Anwendung?
Über Rollen je Organisation (Administration, Recht und Compliance, Management, Fachbereich, Lesen, Auditor, externe Beratung). Jeder Zugriff wird auf dem Server gegen Rolle und Berechtigung geprüft. Jede fachliche Änderung steht mit Person und Zeitpunkt im Audit-Trail, verkettet über SHA-256.

§ 32 Abs. 4 lit. j NISG 2026: Mehr-Faktor-Authentifizierung und gesicherte Kommunikation

Gibt es Zwei-Faktor-Anmeldung für unsere Benutzer?
Ja: Zwei-Faktor-Anmeldung (TOTP), Bestätigung neuer Geräte per E-Mail und widerrufbare Sitzungen. Im Paket Enterprise Single Sign-on (OpenID Connect, SAML) und SCIM, auf Wunsch verpflichtend.

Sind die Konten des Betreibers mit Zwei-Faktor geschützt?
Ja für den administrativen Zugang, das Betreiberkonto der Anwendung und die Konten beim Hosting-Anbieter.

Gibt es gesicherte Kommunikation für Notfälle?
Angabe folgt. Bitte fragen Sie bei security@lexploris.com an.

3. Auftragsverarbeitungsvertrag (AVV)

Version 2.5 · Stand 26.10.2026

zwischen dem **Kunden** gemäß Bestellung oder Angebot (im Folgenden „Verantwortlicher“)

und **Neuralis GmbH i.G.**, Gesellschaft mit beschränkter Haftung in Gründung, Stephansplatz 8/20, 1010 Wien, Österreich (im Folgenden „Auftragsverarbeiter“).

Dieser Vertrag ist Bestandteil jedes Vertrags über die Nutzung von Lexploris (Hauptvertrag: Bestellung oder Angebot samt Allgemeinen Geschäftsbedingungen). Er wird mit dem Hauptvertrag geschlossen; einer gesonderten Unterschrift bedarf es nicht. Auf Wunsch stellen wir eine unterschriebene Fassung bereit.

1. Gegenstand und Dauer

1.1 Der Auftragsverarbeiter stellt dem Verantwortlichen die Anwendung Lexploris als Cloud-Dienst bereit. Dabei verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag regelt die datenschutzrechtlichen Pflichten beider Parteien nach Art. 28 DSGVO.

1.2 Der Vertrag gilt für die Dauer des Hauptvertrags und darüber hinaus, solange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet (Punkt 9).

2. Art, Zweck und Umfang der Verarbeitung

2.1 Zweck ist die Bereitstellung, der Betrieb, die Sicherung und der Support von Lexploris: Rechtsmonitoring, Rechtsregister, Bewertung von Rechtsänderungen, Aufgaben, Nachweise, Berichte und Schnittstellen.

2.2 Art der Verarbeitung: Erheben, Speichern, Ordnen, Auslesen, Abgleichen, Übermitteln an die vom Verantwortlichen berechtigten Personen und Systeme, Bewertung mit Sprachmodellen, Sichern, Wiederherstellen und Löschen.

2.3 Kategorien betroffener Personen und Arten personenbezogener Daten ergeben sich aus **Anlage 1**.

2.4 Anwendung, Datenbank, Dateien und Sicherungen betreibt der Auftragsverarbeiter auf einem gemieteten Server der netcup GmbH in einem Rechenzentrum in Wien, Österreich (Anlage 3). Eine zweite, verschlüsselte Kopie der Sicherungen hält er auf einem eigenen Server in Österreich. Die Sprachmodelle nutzt er bei Mistral AI in der Europäischen Union. Unterauftragsverarbeiter können Daten auch außerhalb der Europäischen Union verarbeiten; das ist in Anlage 3 angegeben und richtet sich nach Punkt 11.

3. Weisungen

3.1 Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Als Weisung gelten der Hauptvertrag, dieser Vertrag sowie die Einstellungen und Handlungen der Benutzerinnen und Benutzer des Verantwortlichen in Lexploris. Weitere Weisungen erteilt der Verantwortliche in Textform.

3.2 Ist der Auftragsverarbeiter durch das Recht der Union oder Österreichs zu einer anderen Verarbeitung verpflichtet, teilt er dies dem Verantwortlichen vorher mit, sofern das Recht dies nicht verbietet.

3.3 Hält der Auftragsverarbeiter eine Weisung für datenschutzwidrig, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

3.4 Gibt der Verantwortliche einer externen Beratung die Rolle „Beratung (Mandat)“, gelten deren Handlungen in Lexploris als Handlungen von Benutzerinnen und Benutzern des Verantwortlichen nach Punkt 3.1. Der Verantwortliche kann diesen Zugang jederzeit beenden. Das Verhältnis zwischen Verantwortlichem und Beratung regeln diese selbst.

4. Vertraulichkeit

Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (§ 6 DSG). Die Verpflichtung gilt auch nach Ende der Tätigkeit.

5. Sicherheit der Verarbeitung

5.1 Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in **Anlage 2** beschrieben sind.

5.2 Die Maßnahmen dürfen dem technischen Fortschritt angepasst werden, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert der Auftragsverarbeiter und teilt sie auf Anfrage mit.

6. Unterauftragsverarbeiter

6.1 Der Verantwortliche genehmigt die in **Anlage 3** genannten Unterauftragsverarbeiter. Die jeweils aktuelle Liste ist unter Unterauftragnehmer veröffentlicht.

6.2 Der Auftragsverarbeiter darf weitere Unterauftragsverarbeiter beauftragen oder bestehende ersetzen, wenn er den Verantwortlichen mindestens 30 Tage vorher in Textform informiert, etwa per E-Mail oder in der Anwendung. Der Verantwortliche kann innerhalb dieser Frist aus datenschutzrechtlichen Gründen widersprechen. Können sich die Parteien nicht einigen, darf der Verantwortliche den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

6.3 Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein gleichwertiges Schutzniveau (Art. 28 Abs. 4 DSGVO) und haftet für dessen Einhaltung.

6.4 Keine Unterauftragsverarbeitung sind Nebenleistungen ohne Zugriff auf Daten des Verantwortlichen, etwa Telekommunikation, sowie die Zahlungsabwicklung durch Stripe, die Stripe für die Vertragsabwicklung mit dem Verantwortlichen in eigener Verantwortung erbringt.

7. Rechte betroffener Personen

7.1 Lexploris ermöglicht dem Verantwortlichen, Daten selbst zu berichtigen, zu löschen und zu exportieren.

7.2 Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst. Soweit der Verantwortliche ein Anliegen nicht selbst erfüllen kann, unterstützt ihn der Auftragsverarbeiter.

8. Unterstützung und Meldung von Verletzungen

8.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei den Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung und Benachrichtigung bei Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

8.2 Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten ohne unangemessene Verzögerung, spätestens **48 Stunden** nach Kenntnis, an die in Lexploris hinterlegte Adresse der Administration. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben werden nachgereicht.

8.3 Der Auftragsverarbeiter ergreift unverzüglich Maßnahmen, um die Verletzung einzudämmen und nachteilige Folgen zu mindern, und dokumentiert sie.

9. Rückgabe und Löschung

9.1 Während der Laufzeit kann der Verantwortliche seine Daten jederzeit selbst exportieren.

9.2 Nach Ende des Hauptvertrags bleibt der Export 30 Tage möglich. Danach löscht der Auftragsverarbeiter die Daten. Sicherungskopien werden im regulären Zyklus überschrieben, spätestens 30 Tage nach der Löschung. Die Löschung bestätigt er auf Anfrage in Textform.

9.3 Gesetzliche Aufbewahrungspflichten des Auftragsverarbeiters, etwa für Rechnungsdaten, bleiben unberührt.

10. Nachweise und Kontrollen

10.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlich sind, insbesondere die aktuelle Fassung der Anlagen 2 und 3.

10.2 Der Verantwortliche oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer darf die Einhaltung nach Vorankündigung von mindestens 14 Tagen prüfen, in der Regel höchstens einmal je Jahr, bei begründetem Anlass auch öfter. Die Prüfung erfolgt vorrangig durch Auskünfte und Unterlagen. Eine Prüfung vor Ort darf den Betrieb und die Vertraulichkeit der Daten anderer Kundinnen und Kunden nicht beeinträchtigen.

10.3 Der Auftragsverarbeiter kann einen angemessenen Ersatz seines Aufwands für Prüfungen vor Ort verlangen, außer die Prüfung ergibt einen wesentlichen Verstoß.

11. Übermittlung in Drittländer

11.1 Daten werden nur in Drittländer übermittelt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

11.2 Die Unterauftragsverarbeiter nach Anlage 3 verarbeiten die Daten in der Europäischen Union. Setzt Mistral AI eigene Dienstleister außerhalb der Europäischen Union ein, stützt sich die Übermittlung auf die Standardvertragsklauseln der Europäischen Kommission (Art. 46 Abs. 2 lit. c DSGVO) im Vertrag mit Mistral AI. Amazon Web Services verarbeitet die Daten in der Region Frankfurt am Main, gehört aber zu einem Konzern mit Sitz in den USA; insoweit gelten der Angemessenheitsbeschluss zum EU-US Data Privacy Framework (Art. 45 DSGVO) und ergänzend die Standardvertragsklauseln im Vertrag mit Amazon Web Services.

11.3 **Ausweichanbieter der KI.** Fällt Mistral AI aus oder liefert es keine brauchbaren Ergebnisse, darf der Auftragsverarbeiter vorübergehend Amazon Bedrock in der Region Frankfurt am Main nutzen (Anlage 3). Der Verantwortliche genehmigt diesen Ausweichanbieter mit diesem Vertrag; einer Ankündigung nach Punkt 6.2 bedarf es dafür nicht. Der Auftragsverarbeiter dokumentiert jede Umschaltung und kehrt zu Mistral AI zurück, sobald dieser wieder zuverlässig arbeitet. Der Verantwortliche kann jederzeit in Textform verlangen, dass die KI-Bewertung für seine Organisation abgeschaltet wird; Lexploris arbeitet dann mit einer regelbasierten Einstufung ohne KI weiter.

12. Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien gelten die Haftungsregeln des Hauptvertrags, soweit Art. 82 DSGVO nicht zwingend anderes vorsieht.

13. Schlussbestimmungen

13.1 Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht dieser Vertrag in Fragen des Datenschutzes vor.

13.2 Änderungen und Ergänzungen bedürfen der Textform.

13.3 Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.

13.4 Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen. Gerichtsstand ist Wien.

Anlage 1 – Betroffene Personen und Datenarten

Der Verantwortliche bestimmt selbst, welche Daten er in Lexploris erfasst. Typischerweise sind betroffen:

Betroffene Personen	Datenarten

Benutzerinnen und Benutzer des Verantwortlichen (Beschäftigte, Organe, beauftragte Beraterinnen und Berater, Auditorinnen und Auditoren)	Name, geschäftliche E-Mail-Adresse, Rolle und Berechtigungen, Bereichszuordnung, Anmeldedaten (Passwort-Hash, Zwei-Faktor-Geheimnis verschlüsselt, bestätigte Geräte, Sitzungen), Spracheinstellung, Benachrichtigungseinstellungen
Zuständige ohne eigenes Konto	Name, Funktion, Zuständigkeit für Bereiche, Aufgaben und Pflichten
Alle in der Anwendung genannten Personen	Entscheidungen, Begründungen, Kommentare, Aufgaben, Fristen, Anhänge, Lesebestätigungen und Einträge im Audit-Trail mit Person und Zeitpunkt
Ansprechpersonen bei Schnittstellen	Namen und Kontaktdaten in Webhook-, Kalender- oder Integrationskonfigurationen

Unternehmens- und Bereichsprofile beschreiben die Organisation (Branche, Standorte, Tätigkeiten) und enthalten in der Regel keine personenbezogenen Daten. Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) und strafrechtlich relevanter Daten (Art. 10 DSGVO) ist nicht Zweck des Dienstes.

Anlage 2 – Technische und organisatorische Maßnahmen

Maßnahmen, die noch nicht vollständig umgesetzt sind, sind als geplant gekennzeichnet. Der Auftragsverarbeiter aktualisiert diese Anlage, sobald sie umgesetzt sind.

Vertraulichkeit

Zutrittskontrolle

- Betrieb auf einem gemieteten Server der netcup GmbH in einem Rechenzentrum in Wien. netcup ist nach ISO/IEC 27001 zertifiziert; Zutritt zum Rechenzentrum regelt der Anbieter.
- Das Rechenzentrum ist an den Vienna Internet Exchange (VIX) angebunden, bezieht Ökostrom aus Wasserkraft und hat einen Schutz gegen DDoS-Angriffe.
- Die zweite Kopie der Sicherungen liegt verschlüsselt auf einem eigenen Server des Auftragsverarbeiters in versperrten Räumlichkeiten in Österreich.

Zugangskontrolle

- Administrativer Zugang nur für namentlich benannte Personen, mit Zwei-Faktor-Anmeldung und persönlichen Schlüsseln.
- Server: Anmeldung per SSH nur mit Schlüssel, ohne Passwort; Schutz vor wiederholten Fehlversuchen; eingehend nur SSH und HTTPS (Firewall). Die Konten beim Hosting-Anbieter sind mit Zwei-Faktor-Anmeldung geschützt.
- Die Sicherungen holt der zweite Server über ein eigenes Konto ab, das nur Sicherungsdateien lesen kann.
- Anmeldung an der Anwendung: Passwörter mit Argon2id gehasht, Mindestanforderungen an Passwörter, Sperre und Verzögerung nach wiederholten Fehlversuchen.
- Zwei-Faktor-Anmeldung (TOTP), Bestätigung neuer Geräte per E-Mail, Sitzungen mit absoluter Laufzeit und Leerlaufzeit, jederzeit widerrufbar.
- Single Sign-on (OpenID Connect, SAML) und Benutzerabgleich per SCIM im Paket Enterprise, auf Wunsch verpflichtend.

Zugriffskontrolle

- Rollen je Organisation (Administration, Recht und Compliance, Management, Fachbereich, Lesen, Auditor, externe Beratung); jeder Zugriff wird auf dem Server gegen Rolle und Berechtigung geprüft.

- API-Schlüssel je Organisation, nur als Hash gespeichert, mit Berechtigungen (Scopes), Zeitpunkt der letzten Nutzung und jederzeitigem Widerruf.
- Gespeicherte Geheimnisse für Schnittstellen werden verschlüsselt.

Trennungskontrolle

- Jede Abfrage der Anwendung ist auf die eigene Organisation beschränkt.
- Zweite Schutzebene: Zeilenrechte (Row Level Security) in PostgreSQL für alle mandantenbezogenen Tabellen.
- Automatische Tests nur mit Demodaten in einer getrennten Testdatenbank. Entwicklung und Testsystem laufen auf einem eigenen System des Auftragsverarbeiters, getrennt vom Betrieb und nur mit Demodaten.

Verschlüsselung

- Übertragung ausschließlich über TLS; HTTP Strict Transport Security. TLS endet auf dem Server des Auftragsverarbeiters; kein Dienstleister sieht die Inhalte dazwischen.
- Sicherungen mit AES-256 verschlüsselt, bevor sie den Server verlassen; den Schlüssel hat nur der Auftragsverarbeiter.

Integrität

Weitergabekontrolle

- Inhalte nur an berechtigte Benutzerinnen und Benutzer; Personenauswahl nur innerhalb der eigenen Organisation.
- Webhooks mit HMAC signiert; Einmal-Links aus E-Mails befristet und nur einmal verwendbar.
- Strenge Content-Security-Policy, Schutz vor Clickjacking und MIME-Sniffing.

Eingabekontrolle

- Audit-Trail mit Person, Zeitpunkt, Aktion und Inhalt jeder fachlichen Änderung, je Organisation als Hash-Kette (SHA-256) verkettet; nachträgliche Änderungen werden erkennbar.
- Rechnungen und abgeschlossene Nachweise werden schreibgeschützt mit Prüfsumme archiviert.
- Jeder Aufruf eines Sprachmodells wird mit Zweck, Modell und Umfang protokolliert.

Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung von Datenbank, Dateien und Archiv, verschlüsselt, mit festgelegter Aufbewahrung: 14 Tage auf dem Server, höchstens 30 Tage als zweite Kopie an einem getrennten Ort in Österreich.
- Dokumentiertes Verfahren zur Wiederherstellung, das regelmäßig getestet wird.
- Container mit Zustandsprüfung und automatischem Neustart; Überwachung der Container und der Abrufläufe mit Alarm bei Ausfällen; öffentliche Statusseite.
- Server-Protokolle höchstens 30 Tage, keine Zugriffsprotokolle mit IP-Adressen.
- Begrenzung der Anfragen je Quelle und Nutzer (Rate-Limits).

Verfahren zur regelmäßigen Überprüfung

- Code-Review und automatische Tests vor jeder Auslieferung, darunter Tests zur Mandantentrennung und zu Berechtigungen.
- Prüfung der Abhängigkeiten auf bekannte Schwachstellen; Abhängigkeiten in festen Versionen.
- Penetrationstest durch externe Prüfer: geplant, noch nicht durchgeführt; danach in regelmäßigen Abständen.
- Prozess für Sicherheitsvorfälle mit Meldung an Verantwortliche binnen 48 Stunden; Kontakt für Schwachstellenmeldungen über security.txt.
- Überprüfung dieser Maßnahmen mindestens jährlich und bei wesentlichen Änderungen.

Datenschutz durch Technikgestaltung

- Nur die für den Dienst nötigen Daten werden erhoben; Profile beschreiben Organisationen, nicht Personen.
- Sprachmodelle bei Mistral AI in der Europäischen Union, ohne Training mit den Daten; bei Störungen vorübergehend Amazon Bedrock in Frankfurt ohne Speicherung (Punkt 11.3). Jede KI-Aussage braucht ein wörtliches, automatisch geprüftes Zitat aus der Quelle. Quelltexte werden als Daten, nicht als Anweisung behandelt; an das Modell gehen keine Namen von Personen aus der Anwendung, soweit sie nicht in Freitexten, hochgeladenen Richtlinien oder deren Dateieigenschaften (Autor, „Zuletzt geändert von“) oder im Spruch hochgeladener Bescheide des Verantwortlichen enthalten sind.
- Keine Tracking- oder Werbedienste.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung
netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, Deutschland	Server für Anwendung, Datenbank, Dateien und Sicherungen	Rechenzentrum in Wien, Österreich
Mistral AI SAS, 15 rue des Halles, 75001 Paris, Frankreich	Sprachmodelle für Bewertung, Zusammenfassung, Richtlinienprüfung, Auflagen aus Bescheiden und Assistent; kein Training mit den Daten	Europäische Union; Dienstleister außerhalb der EU nur mit Standardvertragsklauseln (Punkt 11.2)
webgo GmbH, Heidenkampsweg 81, 20097 Hamburg, Deutschland	Versand von System-E-Mails, Postfach	Deutschland
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg (Amazon Bedrock) – **nur als Ausweichanbieter bei Störungen-**, Punkt 11.3	Sprachmodelle wie Mistral AI, ohne Speicherung und Training	Region Frankfurt am Main (eu-central-1); Konzern mit Sitz in den USA (Punkt 11.2)

Die jeweils aktuelle Liste veröffentlichen wir unter Unterauftragnehmer.

4. Unterauftragnehmer

Version 2.3 · Stand 26.10.2026

Für den Betrieb von Lexploris setzen wir die folgenden Dienstleister ein. Soweit sie personenbezogene Daten in unserem Auftrag verarbeiten, bestehen Verträge nach Art. 28 Abs. 4 DSGVO. Über neue oder geänderte Unterauftragsverarbeiter informieren wir Kundinnen und Kunden mindestens 30 Tage im Voraus (Punkt 6 des Auftragsverarbeitungsvertrags).

Hosting. Anwendung, Datenbank, Dateien und Sicherungen laufen auf einem Server, den wir bei netcup in einem Rechenzentrum in Wien mieten. Eine zweite, verschlüsselte Kopie der Sicherungen holt ein eigener Server des Betreibers in Österreich ab. Die Sprachmodelle nutzen wir bei Mistral AI in der EU.

Unterauftragsverarbeiter

Dienstleister	Leistung	Verarbeitete Daten	Ort der Verarbeitung
netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, Deutschland	Server für Anwendung, Datenbank, Dateien und Sicherungen (zertifiziert nach ISO/IEC 27001)	alle Daten in Lexploris	Rechenzentrum in Wien, Österreich
Mistral AI SAS, 15 rue des Halles, 75001 Paris, Frankreich	Sprachmodelle für Bewertung, Zusammenfassung, Prüfung interner Richtlinien und Assistent; kein Training mit unseren Daten	Rechtstexte, Unternehmens- und Bereichsprofile, Entscheidungen und Fragen der Organisation; für Richtlinienprüfung und Assistent auch interne Richtlinien mit Dateieigenschaften, Stellungnahmen und Aufgabenbeschreibungen	Rechenzentren in der EU; Dienstleister von Mistral AI außerhalb der EU nur mit Standardvertragsklauseln
webgo GmbH, Heidenkampsweg 81, 20097 Hamburg, Deutschland	Versand von System-E-Mails (Bestätigungscodes, Einladungen, Benachrichtigungen, Fristerinnerungen) und des Newsletters, Postfach für Anfragen und Nameserver für die Domain (DNS)	Name und E-Mail-Adresse der Empfängerinnen und Empfänger, Inhalt der Nachricht	Deutschland

Ausweichanbieter für Störungen der KI

Fällt Mistral AI aus oder liefert es keine brauchbaren Ergebnisse, können wir vorübergehend auf den folgenden Anbieter wechseln. Er ist vorab genehmigt (Anlage 3 des Auftragsverarbeitungsvertrags) und im Normalbetrieb nicht im Einsatz.

Dienstleister	Leistung	Ort der Verarbeitung
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg (Amazon Bedrock)	Sprachmodelle wie oben; nach Angaben von Amazon keine Speicherung, kein Training und keine Weitergabe an den Modellhersteller	Region Frankfurt am Main (eu-central-1); Amazon gehört zu einem Konzern mit Sitz in den USA

Weitere Dienstleister ohne Zugriff auf Inhalte

Dienstleister	Leistung	Ort der Verarbeitung
Internet Security Research Group (Let's Encrypt), San Francisco, USA	Ausstellung der TLS-Zertifikate; erhält nur den Namen der Domain, keine Daten von Besucherinnen und Besuchern	USA

Eigenständig Verantwortliche

Die folgenden Anbieter verarbeiten Daten in eigener Verantwortung, wenn Sie die jeweilige Funktion nutzen. Sie sind keine Unterauftragsverarbeiter.

Anbieter	Funktion	Ort der Verarbeitung
Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland	Zahlungsabwicklung, Rechnungen, Kundenportal	EU, teilweise USA
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	Anmeldung mit Google-Konto (optional, sofern angeboten)	EU und USA
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Anmeldung mit Microsoft-Konto (optional, sofern angeboten)	EU und USA
Kanzlei, an die Sie eine Anfrage richten	Beantwortung Ihrer Frage im Einzelfall	je nach Kanzlei

Datenquellen

Lexploris ruft Rechtsdaten von öffentlichen Stellen ab: Rechtsinformationssystem des Bundes (Bundeskanzleramt), EUR-Lex (Amt für Veröffentlichungen der Europäischen Union) und Parlament Österreich, für Deutschland und die Schweiz, soweit aktiviert, auch die amtlichen Portale des Bundes (NeuRIS, gesetze-im-internet.de, Fedlex). Dabei werden keine personenbezogenen Daten unserer Kundinnen und Kunden übermittelt.

Fragen zu dieser Liste richten Sie bitte an kontakt@lexploris.com.