Sicherheit & Compliance

Technisches Datenblatt: Datensicherheit & Infrastruktur

LexLogik - Die souveräne Lösung für Berufsgeheimnisträger

Dieses Dokument fasst die technisch-organisatorischen Schutzmassnahmen der LexLogik-Plattform zusammen. Für Schweizer Kanzleien adressiert es insbesondere die Anforderungen aus Art. 321 StGB und Art. 13 BGFA. Datenblatt und AV-Muster stehen unten zum Download bereit.

1. Quick-Check für die IT-Prüfung

- Cloud-Modell: 100 % Private Cloud (Keine Nutzung von US-Hyperscalern wie AWS/Azure/Google).
- Verschlüsselung: TLS 1.3 (Transport) / AES-256 (Ruhende Daten & Session-Partitionen).
- Speicher-Paradigma: Zero-Retention (Keine dauerhafte Speicherung von Inhaltsdaten).
- KI-Infrastruktur: Lokales Inferencing auf eigener Hardware (Keine Drittanbieter-APIs / No-OpenAI).
- Serverstandort: Nürnberg & Falkenstein, Deutschland.
- Compliance & Berufsgeheimnis: Ausrichtung auf Art. 321 StGB (strafrechtlicher Schutz des Berufsgeheimnisses), Art. 13 BGFA und revDSG.

2. Hosting & Digitale Souveränität

LexLogik setzt für die Kernbearbeitung überwiegend auf europäische Infrastruktur und eigene Server in Deutschland; Hilfsdienste mit Auslandsbezug sind dokumentiert und auf das technisch Notwendige begrenzt.

- Infrastruktur: Betrieb auf dedizierter Hardware in deutschen Hochsicherheits-Rechenzentren (Partner: Hetzner Online GmbH).
- Zertifizierung (Hosting): Die von uns genutzten Rechenzentren des Partners Hetzner Online GmbH sind ISO 27001-zertifiziert.
- Netzwerksicherheit: Mehrstufige Firewall-Architektur. Administrativer Zugriff erfolgt ausschliesslich über verschlüsselte VPN-Tunnel und Multi-Faktor-Authentifizierung (MFA).

3. Der LexLogik Datenzyklus (Zero-Retention)

Unsere Architektur ist darauf ausgelegt, das Risiko eines Datendiebstahls durch die konsequente Vermeidung von dauerhafter Speicherung technisch zu minimieren.

- Transport: Ende-zu-Ende-Verschlüsselung via TLS 1.3.
- Bearbeitung: Die Dokumenten-Optimierung und Textextraktion erfolgt in flüchtigen RAM-Instanzen bzw. auf temporär verschlüsselten Session-Partitionen.
- Automatisierter Purge-Prozess: Unmittelbar nach Abschluss der Bearbeitung und Bereitstellung des Downloads werden Quelldatei und Ergebnis unwiderruflich gelöscht. Es werden keine Backups von Mandantendaten erstellt.
- Metadaten-Trennung: Inhaltsdaten werden strikt von administrativen Metadaten (z. B. Zeitstempel für das Audit-Logging) getrennt.

4. Souveräne KI-Architektur (No-API Policy)

- Lokales Modell-Hosting: Unsere dualen OCR-Engines und die Legal-KI arbeiten als containerisierte Instanzen direkt auf unserer Hardware in Deutschland.
- Kein KI-Training: Kundendaten werden zu keinem Zeitpunkt für das Training oder die Verbesserung von KI-Modellen verwendet. Unsere Modelle sind fest eingebettet und werden nicht durch Nutzerdaten verändert.

5. Compliance & Rechtlicher Rahmen

LexLogik wurde speziell für Berufsgeheimnisträger entwickelt - mit Fokus auf Art. 321 StGB und die Pflichten aus Art. 13 BGFA.

- Art. 321 StGB & Art. 13 BGFA: Die technischen Schutzmassnahmen unterstützen die Wahrung des rechtsanwaltlichen Berufsgeheimnisses bei der Einbindung von Hilfspersonen und IT-Dienstleistern.
- Personal-Compliance: Sämtliche Mitarbeitende mit Zugriff auf die Systemadministration sind schriftlich auf das Datengeheimnis sowie auf die Pflichten gemäss Art. 321 StGB und revDSG verpflichtet.

6. Mandantentrennung & Logische Isolation

- Mandantentrennung: Die Verarbeitung erfolgt in strikt voneinander isolierten Container-Instanzen. Datenströme verschiedener Nutzer können sich auf technischer Ebene zu keinem Zeitpunkt vermischen.
- Der Zugriff auf Verarbeitungsressourcen wird durch ein granulares Berechtigungssystem gesteuert - jeder Account erhält ausschliesslich die Rechte, die für seine Aufgabe zwingend erforderlich sind.

7. Verfügbarkeit & Resilienz

- Redundanz: Durch die Nutzung der Standorte Nürnberg und Falkenstein ist eine geografische Redundanz gegeben. Fällt ein Standort aus, bleibt der Dienst über den zweiten Standort verfügbar.
- DDoS-Schutz: Die Infrastruktur ist gegen gezielte Überlastungsangriffe geschützt - die Erreichbarkeit des Dienstes bleibt auch unter Angriffsbedingungen gewährleistet.

8. Incident Management & Auditing

- Incident Response: Es besteht ein definierter Prozess zur Identifikation, Meldung und Behebung von Sicherheitsvorfällen gemäss Art. 33 DSGVO.
- Logging: System-Events (Logins, API-Calls) werden revisionssicher protokolliert, um Missbrauch zu verhindern. Wichtig: Diese Logs enthalten ausschliesslich technische Metadaten, niemals Inhaltsdaten aus Ihren Dokumenten.

9. Zero-Access-Policy für den Support

- Administrativer Ausschluss: Unsere Mitarbeiter haben technisch keinen Einblick in die flüchtigen Session-Inhalte während der Verarbeitung. Support-Zugriffe auf Nutzerkonten erfolgen ausschliesslich nach expliziter Freigabe durch den Kunden und werden lückenlos dokumentiert.

Ansprechpartner für technische Rückfragen

Clemens Schmid
E-Mail: info@lexlogik.com

Dokumenten-ID: LX-SEC-2026-V2.2
Stand: Juni 2026
Gültigkeit: Alle aktuellen Instanzen (Counsel, Professional, Enterprise)