Security & compliance

Teknisk datablad: datasikkerhet og infrastruktur

LexLogik - den suverene løsningen for taushetsplikt

Revisjonsnotat: Dette dokumentet oppsummerer de tekniske og organisatoriske tiltakene (TOM-er) til LexLogik-plattformen. For å forenkle due diligence har du direkte tilgang nedenfor til det utskrivbare faktabladet og gjeldende mal for databehandleravtale (PDF), inkludert tekniske vedlegg.

1. Rask sjekk for IT-gjennomgang

- Skymodell: 100 % privat sky (ingen bruk av US hyperscalere som AWS/Azure/Google).
- Kryptering: TLS 1.3 (under overføring) / AES-256 (data i ro og øktpartisjoner).
- Lagringsparadigme: Zero-Retention (ingen vedvarende lagring av innholdsdata).
- KI-infrastruktur: Lokal inferens på egen maskinvare (ingen tredjeparts-API-er / ingen OpenAI).
- Serverlokasjoner: Nürnberg og Falkenstein, Tyskland.
- Samsvar: tilpasset GDPR og advokatens taushetsplikt.

2. Hosting og digital suverenitet

LexLogik er designet for å holde kjernebehandling utenfor virkeområdet til ikke-europeiske jurisdiksjoner, inkludert US CLOUD Act.

- Infrastruktur: Drift på dedikert maskinvare i tyske høysikkerhets datasentre (partner: Hetzner Online GmbH).
- Sertifisering (hosting): Datasentralene vi bruker fra hostingpartner Hetzner Online GmbH er sertifisert etter ISO 27001.
- Nettverkssikkerhet: Flerlags brannmurarkitektur. Administrativ tilgang kun via krypterte VPN-tunneler og flerfaktorautentisering (MFA).

3. LexLogik datasyklus (zero-retention)

Arkitekturen vår er designet for å minimere risikoen for datatyveri ved teknisk å unngå vedvarende lagring.

- Transport: Ende-til-ende-kryptering via TLS 1.3.
- Behandling: Dokumentoptimalisering og tekstuttrekking kjører i flyktige RAM-instanser eller på midlertidig krypterte øktpartisjoner.
- Automatisert sletting: Umiddelbart etter at behandlingen er fullført og nedlastingen er tilgjengelig, slettes kildefil og resultat uten gjenoppretting. Ingen sikkerhetskopier av klientdata opprettes.
- Metadataseparasjon: Innholdsdata er strengt adskilt fra administrativ metadata (f.eks. tidsstempler for revisjonslogging).

4. Suveren KI-arkitektur (ingen API-policy)

I motsetning til standardløsninger overfører ikke LexLogik data til eksterne KI-leverandører.

- Lokal modellhosting: De duale OCR-motorene og juridisk KI kjører som containeriserte instanser direkte på maskinvaren vår i Tyskland.
- Ingen KI-trening: Kundedata brukes aldri til å trene eller forbedre KI-modeller. Alle modeller er statisk forhåndstrent.

5. Samsvar og juridisk rammeverk

LexLogik er utviklet for taushetspliktige miljøer, med fokus på GDPR og kravene i advokatloven.

- Taushetsplikt: De tekniske sikkerhetstiltakene støtter overholdelse av advokatens konfidensialitet ved involvering av tjenesteleverandører. De tekniske tiltakene støtter advokatens taushetsplikt i henhold til domstolloven § 218 og advokatforskriften kapittel 12.
- Personaloverholdelse: Alt personale med tilgang til systemadministrasjon er kontraktsmessig bundet til datahemmelighet og de spesielle pliktene under GDPR.

6. Klientisolasjon og logisk separasjon

- Tenanteisolasjon: Behandling kjører i strengt isolerte containerinstanser. Datastier for ulike brukere kan aldri blandes på teknisk nivå.

- Logisk tilgangskontroll: Tilgang til behandlingsressurser styres av en granulær tillatelsesmodell basert på minste privilegium.

7. Tilgjengelighet og motstandsdyktighet

- Redundans: Bruk av Nürnberg- og Falkenstein-nettsteder gir geografisk redundans. Hvis ett nettsted svikter, forblir tjenesten tilgjengelig via det andre.
- DDoS-beskyttelse: Infrastrukturen er skjermet av spesialiserte skrubbingssentre mot distribuerte tjenestenektangrep for å holde tjenesten pålitelig tilgjengelig for kontordrift.

8. Hendelseshåndtering og revisjon

- Hendelsesrespons: Det er en definert prosess for å identifisere, rapportere og utbedre sikkerhetshendelser i samsvar med GDPR art. 33.
- Logging: Systemhendelser (innlogginger, API-kall) registreres på en revisjonsegnet måte for å avskrekke misbruk. Viktig: disse loggene inneholder bare teknisk metadata - aldri innholdsdata fra dokumentene dine.

9. Policy for nulltilgang til support

- Administrativ eksklusjon: Personalet vårt har ingen teknisk innsikt i flyktig øktinnhold under behandling. Supporttilgang til brukerkontoer skjer bare etter eksplisitt kundegodkjenning og er fullt dokumentert.

Kontakt for tekniske henvendelser

Clemens Schmid
E-post: info@lexlogik.com

Dokument-ID: LX-SEC-2026-V2.2
Per: June 2026
Gjelder for: Alle gjeldende instanser (Counsel, Professional, Enterprise)