Security & compliance

Fiche technique : sécurité des données et infrastructure

LexLogik - La solution souveraine pour les détenteurs du secret professionnel

Vous trouverez ici tous les détails sur nos mesures techniques et organisationnelles (TOM) ainsi que les bases juridiques de notre traitement des données.

1. Contrôle rapide pour l'audit informatique

- Modèle cloud : 100 % Private Cloud (aucun recours aux hyperscalers américains tels qu'AWS/Azure/Google).
- Chiffrement : TLS 1.3 (transport) / AES-256 (données au repos & partitions de session).
- Paradigme de stockage : Zero-Retention (aucun stockage permanent des données de contenu).
- Infrastructure IA : inférence locale sur notre propre matériel (aucune API tierce / no-OpenAI).
- Localisation des serveurs : Nuremberg & Falkenstein, Allemagne.
- Conformité : alignée sur le RGPD et le secret professionnel (CNB).

2. Hébergement & souveraineté numérique

Le traitement principal s'effectue exclusivement sur notre propre matériel en Allemagne - en dehors du champ d'application du US Cloud Act.

- Infrastructure : exploitation sur matériel dédié dans des centres de données haute sécurité en Allemagne (partenaire : Hetzner Online GmbH).
- Certification (hébergement) : les centres de données de notre partenaire Hetzner Online GmbH sont certifiés ISO 27001.
- Sécurité réseau : architecture pare-feu multi-niveaux. L'accès administratif s'effectue exclusivement via des canaux chiffrés.

3. Le cycle de données LexLogik (Zero-Retention)

Notre architecture est conçue pour minimiser le risque de vol de données en évitant systématiquement le stockage permanent.

- Transport : chiffrement de bout en bout via TLS 1.3.
- Traitement : l'optimisation des documents et l'extraction de texte s'effectuent dans des instances RAM volatiles ou sur des disques temporaires chiffrés.
- Processus de purge automatisé : immédiatement après le traitement et la mise à disposition du téléchargement, le fichier source et le résultat sont supprimés de manière irréversible. Aucune sauvegarde des données clients n'est créée.
- Séparation des métadonnées : les données de contenu sont strictement séparées des métadonnées administratives (p. ex. horodatages pour l'audit-logging).

4. Architecture IA souveraine (politique no-API)

- Hébergement local des modèles : nos moteurs OCR doubles et l'IA juridique fonctionnent comme instances conteneurisées directement sur notre propre infrastructure en Allemagne.
- Aucun entraînement IA : les données clients ne sont à aucun moment utilisées pour l'entraînement ou l'amélioration des modèles d'IA. Nos modèles sont fixes et ne sont pas modifiés par les données des utilisateurs.

5. Conformité & cadre juridique

LexLogik a été conçu pour les détenteurs du secret professionnel, avec un accent sur le RGPD et les exigences du secret professionnel de l'avocat.

- CNB : les mesures techniques soutiennent le respect du secret professionnel lors de l'intervention de prestataires.
- Conformité du personnel : les collaborateurs ayant accès à l'administration système sont tenus au secret des données conformément au RGPD.

6. Séparation des clients & isolation logique

- Séparation des clients : le traitement s'effectue dans des instances conteneur strictement isolées. Les flux de données de différents utilisateurs ne peuvent à aucun moment se croiser au niveau technique.
- L'accès aux ressources de traitement est contrôlé par un système de permissions granulaire - chaque compte reçoit uniquement les droits nécessaires à sa fonction.

7. Disponibilité & résilience

- Redondance : l'utilisation des sites de Nuremberg et Falkenstein assure une redondance géographique. En cas de défaillance d'un site, le service reste disponible via le second site.
- Protection DDoS : l'infrastructure est protégée contre les attaques ciblées par saturation - la disponibilité du service est maintenue même en cas d'attaque.

8. Gestion des incidents & audit

- Réponse aux incidents : il existe un processus défini pour l'identification, la notification et la résolution des incidents de sécurité conformément à l'art. 33 RGPD.
- Journalisation : les événements système (connexions, appels API) sont consignés de manière auditables pour prévenir les abus. Ces journaux ne contiennent que des métadonnées techniques - jamais de contenu de documents.

9. Politique zéro accès pour le support

- Exclusion administrative : nos employés n'ont techniquement aucun accès aux contenus de session volatils pendant le traitement. Les accès au support sur les comptes utilisateurs s'effectuent uniquement après autorisation explicite du client et sont intégralement documentés.

Contact pour les questions techniques

Clemens Schmid
E-Mail: info@lexlogik.com

Identifiant du document: LX-SEC-2026-V2.2
Version: juin 2026
Validité: Toutes les instances actuelles (Counsel, Professional, Enterprise)