Anlage I · Kanzlei-Briefing Technisch-organisatorische Maßnahmen (TOM)

Anlage zum Plattform-Anbindungsvertrag (**`KANZLEI_VERTRAG.md`**) sowie Bezugsdokument zur Joint-Controller-Vereinbarung (Anlage A)

Stand: April 2026

Zweck dieser Anlage

Diese Anlage gibt der Kanzlei einen kompakten Überblick über die technisch-organisatorischen Maßnahmen (TOM), die LWYRUP für die Verarbeitung von Mandatsdaten innerhalb der Plattform-Phase einsetzt. Sie ist nicht erschöpfend – die internen Detail-Konzepte (insbesondere `SECURITY.md`) bleiben aus Sicherheitsgründen bei LWYRUP. Die hier dargestellten Eckpfeiler reichen aus, damit die Kanzlei ihre eigene TOM-Dokumentation und ihre eigenen Datenschutz-Pflichten konsistent gestalten kann.

1. Verschlüsselungsarchitektur (Zero Knowledge)

- Inhalte werden auf dem Endgerät des Mandanten erzeugt und dort vor jeder Übertragung verschlüsselt.
- LWYRUP-Server speichert ausschließlich Chiffrate und unkritische Routing-Metadaten (Account-ID, Bundesland, Kanzlei-Zuordnung, Status).
- Algorithmen:
  - AES-256-GCM für die App→Server-Verschlüsselung,
  - X25519-Sealed-Box für die Server→Empfänger-Verschlüsselung (Multi-Recipient gegen den Public Key der Kanzlei und – soweit eingebunden – des LWYRUP-Legal-Teams).
- Schlüsselableitung über HKDF-SHA256.
- Der private Schlüssel des Mandanten verbleibt im Endgerät (iOS Keychain mit `AfterFirstUnlockThisDeviceOnly`); LWYRUP hat keine Kopie und kann den Schlüssel nicht wiederherstellen.

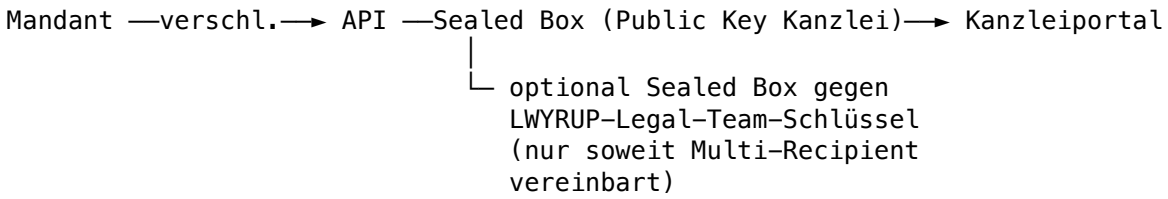
2. Schlüsselmaterial der Kanzlei

- Die Kanzlei erhält bei Onboarding ein eigenes X25519-Schlüsselpaar. Den privaten Schlüssel erhält ausschließlich die Kanzlei; LWYRUP speichert ihn nicht.
- Den öffentlichen Schlüssel der Kanzlei verwendet die Plattform als Empfänger-Schlüssel der Multi-Recipient-Verschlüsselung („Anwalt erhält jede Mandanten-Nachricht für sich verschlüsselt").
- Die Kanzlei sichert ihren privaten Schlüssel in einem geeigneten Schlüsseldienst (HSM, Passwortmanager mit Backup; nicht in Klartext-Dateien). Verlust des Schlüssels führt zum endgültigen Verlust des Zugriffs auf bisherige Chiffrate.

3. Zugang zum Kanzleiportal

- Authentifizierung über ein personenbezogenes X-Lawyer-Token; geteilte Logins sind unzulässig.
- Token wird ausschließlich im `Authorization`-Header übertragen (TLS 1.2+, App Transport Security).
- Token-Rotation: jederzeit über die Kanzleiportal-Einstellungen oder bei Sicherheitsverdacht durch LWYRUP.
- Audit-Log über alle Zugriffe – Aufbewahrung gemäß `VVT.md` B.14 (90 Tage).

4. Datenfluss in der Plattform-Phase



Routing-Metadaten (Bundesland, Produkt-Slug, Kanzlei-ID, Fall-Status) liegen klartextlich vor – sie sind für die Verteilungs- und Workflow-Logik notwendig.

5. Hosting und Standort

- Sämtliche Verarbeitung erfolgt in der Europäischen Union.
- Hosting der API und des Kanzleiportals: ALL-INKL.COM – Neue Medien Münnich (Deutschland).
- KI-Pipeline und Datenexport-Worker: BrazenTellurite GmbH (EU).
- OTP-Versand-Worker: Hetzner Online GmbH (Helsinki, Finnland), Sipgate AG (Düsseldorf, Deutschland).
- Push-Versand: Apple Push Notification Service (Irland) und Firebase Cloud Messaging (Irland).
- Kein Drittlandtransfer und keine SCC-Konstruktionen.

6. Backups und Verfügbarkeit

- Verschlüsselte Backups, Aufbewahrung 3 Jahre rolling.
- Regelmäßige Restore-Tests durch LWYRUP.
- Kein Punkt-Löschen in Backups – Vertraulichkeit bleibt durch Crypto-Shredding gewahrt.

7. Trennung Routing ↔ Inhalte

- Routing-Metadaten werden in DB1 in eigenen Tabellen gehalten, räumlich getrennt von verschlüsselten Inhalts-Blobs.
- Admin-Personal sieht niemals entschlüsselte Mandatsinhalte.

8. Pseudonymisierung abhängiger Personen

- Daten von in einer Bedarfsgemeinschaft genannten Dritten werden mittels HMAC pseudonymisiert. Der HMAC-Schlüssel liegt ausschließlich auf dem Endgerät des Mandanten.

9. Logging und Monitoring

- Sicherheits-Audit-Log: 12 Monate.
- Standard-Logs: 30 Tage.
- Logs enthalten keine Klartext-PII; PII-Logging-Audit ist Bestandteil der Release-Checkliste.

10. Erwartungen an die Kanzlei

Die Kanzlei stellt sicher, dass

- der eigene private Schlüssel sicher verwahrt wird und vertraulich bleibt,
- Zugriffe auf das Kanzleiportal nur durch namentlich benannte, zur Vertraulichkeit verpflichtete Personen erfolgen,
- ausgeschiedene Mitarbeitende und verlorene Geräte unverzüglich zu Token-Sperrung gemeldet werden (`KANZLEI_VERTRAG.md` § 9 Abs. 2),
- die eigenen IT-Systeme nach dem Stand der Technik abgesichert sind (Aktualisierung, Endgeräte-Verschlüsselung, Berechtigungsmanagement, Zwei-Faktor-Authentisierung dort, wo vom Anbieter angeboten),
- Mandatsdaten, die aus der Plattform in die kanzlei-eigene Aktenführung übernommen werden, in den dortigen Systemen einem Schutzniveau unterliegen, das dem hier dargestellten mindestens entspricht.

Zur Kenntnis genommen

Mit Unterzeichnung der Hauptvereinbarung (`KANZLEI_VERTRAG.md`) bestätigt die Kanzlei, diese Anlage zur Kenntnis genommen und ihre Erwartungen aus Abschnitt 10 angenommen zu haben.

Version	Datum	Änderung
0.1	2026-04-30	Erstfassung der Kanzlei-fassung des TOM-Briefings, abgestimmt auf SECURITY.md ohne Hardening-Backlog.
1.0	2026-05-02	Freigabe

Hinweis: Dieses Dokument ist eine kanzleirelevante Kurzfassung; die vollständige interne TOM-Dokumentation (`SECURITY.md`) bleibt bei LWYRUP und wird nicht herausgegeben.