Technische und organisatorische Maßnahmen (TOM)

Sentinel System / zentrale Sentinel-Infrastruktur gemäß Art. 32 DSGVO

Fassung 1.0 – Stand: 09.10.2026

Hinweis: Diese Fassung dokumentiert den aktuellen technischen und organisatorischen Stand. Als offen markierte Verifikationen sind keine bestätigten Maßnahmen.

1. Zweck und Geltungsbereich

Diese technischen und organisatorischen Maßnahmen beschreiben die grundlegenden Sicherheitsmaßnahmen für die von Sentinel System bereitgestellten Dienste und die gemeinsam genutzte technische Infrastruktur der Sentinel-Welt.

Die Sentinel-Welt besteht aus technisch getrennten Diensten und Produktinstanzen. Abhängig vom jeweiligen Produkt und Bereitstellungsmodell können Dienste auf dedizierten virtuellen Maschinen oder als voneinander getrennte Anwendungen auf einer gemeinsamen Serverinstanz betrieben werden.

Produktspezifische Maßnahmen, insbesondere für den Virtuellen Bürger-Schreibtisch, die Schuldnerberatung, die Sentinel Prozessverwaltung, Kommunikationsdienste und weitere Fachanwendungen, werden ergänzend in produktspezifischen Anlagen dokumentiert.

Die Maßnahmen dienen insbesondere der Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sowie der Wiederherstellbarkeit und regelmäßigen Überprüfung der Wirksamkeit der eingesetzten Schutzmaßnahmen.

2. Infrastruktur und Hosting

Die produktive Sentinel-Infrastruktur wird auf Serverinfrastruktur von Hetzner in Nürnberg, Deutschland, betrieben.

Zum dokumentierten technischen Grundaufbau gehören insbesondere:

- Ubuntu-basierte Serversysteme
- Docker Engine und Docker Compose für containerisierte Dienste
- hostbasierte Firewall-Regeln
- fail2ban zur automatisierten Reaktion auf auffällige beziehungsweise wiederholte fehlgeschlagene Zugriffsversuche
- vorgeschaltete TLS-/Reverse-Proxy-Strukturen
- getrennte Anwendungsdienste und interne Ports
- persistente, dienstbezogene Datenspeicher
- kontrollierte Kommunikationswege zwischen Anwendungen und zentralen Diensten

Die öffentlich erreichbaren Dienste werden nicht dadurch voneinander getrennt, dass lediglich unterschiedliche Benutzeroberflächen dargestellt werden. Die Sentinel-Architektur sieht eine technische Trennung auf Anwendungs-, Dienst- und – abhängig vom Produkt – Instanzebene vor.

Status: UMGESETZT / produktspezifische Ausprägung gesondert dokumentieren

3. Trennung von Anwendungen und Mandanten

Sentinel verwendet abhängig vom Produkt unterschiedliche Isolationsmodelle.

Bei der Sentinel Prozessverwaltung kann die Bereitstellung als dedizierte Cloud-Instanz je Kanzlei erfolgen. Die vorliegende technische Produktdokumentation beschreibt hierfür unter anderem eigene Laufzeit- und Datenbereiche sowie eine eigene Datenbank beziehungsweise eigene persistente Verzeichnisse.

Andere Dienste der Sentinel-Welt können auf derselben Serverinstanz betrieben werden, bleiben jedoch als eigenständige Anwendungen beziehungsweise Dienste getrennt.

Der Virtuelle Bürger-Schreibtisch wird gegenwärtig gemeinsam mit Sentinel System auf einer Serverinstanz betrieben und als eigenständiger Dienst über einen separaten internen Anwendungsport (8104) bereitgestellt.

Die Trennung einzelner Bürgerkonten erfolgt dort zusätzlich auf Anwendungsebene. Fachobjekte werden einer account_id zugeordnet; Zugriffsentscheidungen werden serverseitig anhand der jeweiligen Konto-, Rollen- und Freigabeberechtigungen getroffen.

Die Sicherheit eines Mandanten wird damit nicht allein durch eine unterschiedliche URL, Benutzeroberfläche oder Portnummer begründet.

Status: UMGESETZT; Dateisystem-, Container- und Datenbankgrenzen vor Veröffentlichung abschließend dokumentieren

4. Transportverschlüsselung und Netzwerksicherheit

Öffentlich erreichbare Sentinel-Dienste werden über TLS bereitgestellt.

Interne Anwendungsports werden über vorgeschaltete Web-/Reverse-Proxy-Dienste angebunden und nicht als unmittelbare öffentliche Anwendungszugänge verwendet.

Die Host-Firewall verwendet die Default-Policies INPUT DROP und FORWARD DROP. Nicht mehr benötigte historische Freigaben für 21, 3000, 5432, 7860 und 8080 wurden entfernt.

Für Docker-Ingress besteht eine persistente DOCKER-USER-Allowlist. Neue externe Containerverbindungen sind ausschließlich für die bewusst veröffentlichten Originalports 80, 443 und 2022 zugelassen.

Der administrative SSH-Zugang verwendet keine Passwortauthentisierung, maximal drei Authentisierungsversuche und ein UFW-Verbindungsrate-Limit.

Für den Bürger-Schreibtisch terminiert Caddy TLS, erzwingt HTTP-zu-HTTPS und setzt HSTS. Port 8104 ist weder an Loopback noch an die öffentliche Host-IP gebunden.

Status: TECHNISCH VERIFIZIERT AM 09.10.2026; administrative Root-Key-Nutzung bleibt gesondert organisatorisch zu bewerten

5. Identitäts- und Zugangsmanagement

Sentinel setzt abhängig vom jeweiligen Dienst mehrere Authentisierungsmechanismen ein. Hierzu gehören insbesondere:

- Passwortauthentisierung
- Passkeys/WebAuthn
- sitzungsgebundene Authentisierung
- Rollen- und Berechtigungssysteme
- zeitlich beziehungsweise funktional begrenzte Einladungen
- Wiederherstellungsverfahren
- Widerruf aktiver Sitzungen
- produktbezogene Freigabemechanismen

Passkeys des Bürger-Schreibtischs verwenden verpflichtende Benutzerverifikation. Herausforderungen werden zeitlich begrenzt und an die vorgesehene Anwendung beziehungsweise Origin/RP-ID gebunden.

Recovery-Codes werden nicht im Klartext als wiederverwendbare Zugangsdaten gespeichert. Erfolgreiche Wiederherstellungsvorgänge führen zur Invalidierung bestehender Sitzungen.

Rollenänderungen, Kontosperren und das Entfernen von Benutzern führen bei entsprechend geschützten Funktionen zum Entzug bestehender Berechtigungen und Sitzungen.

Status: Bürger-Schreibtisch: automatisiert getestet

6. Berechtigungs- und Zugriffskontrolle

Der Zugriff auf personenbezogene Inhalte erfolgt nach dem Prinzip der erforderlichen Berechtigung.

Die Anwendungen unterscheiden insbesondere zwischen:

- Kontoinhabern
- Administratoren beziehungsweise Managern
- Mitgliedern
- ausschließlich leseberechtigten Benutzern
- externen beziehungsweise besonders freigegebenen Fachrollen

Berechtigungen werden serverseitig geprüft.

Die bloße Kenntnis einer Objekt-ID darf keinen Zugriff auf Objekte eines anderen Kontos ermöglichen.

Beim Bürger-Schreibtisch werden entsprechende Account-, Matter-, Gruppen- und IDOR-Szenarien durch automatisierte Regressionstests überprüft.

Administrative Funktionen werden von normalen Benutzerfunktionen getrennt.

7. Dokumenten- und Dateisicherheit

Dokumente werden objekt- und kontobezogen verarbeitet.

Zu gespeicherten Dateien können insbesondere folgende technische Informationen geführt werden:

- Kontozuordnung
- Objektzuordnung
- MIME-Typ
- Dateigröße
- kryptografischer Hash
- Speicherstatus
- Freigabestatus
- Löschstatus
- Verschlüsselungsmodus

Originaldokumente werden bei Analyse-, OCR-, Konvertierungs- und vergleichbaren Verarbeitungsschritten soweit vorgesehen erhalten, sodass abgeleitete Fassungen nicht unbemerkt das Original ersetzen.

Dateizugriffe unterliegen denselben Konto- und Berechtigungsprüfungen wie die zugehörigen Fachobjekte.

Der Standard-Safe wird durch die LUKS2-Blockverschlüsselung des Produktivvolumes und restriktive Dateirechte geschützt; dies wird nicht als kryptografische Betreiberblindheit dargestellt.

Der getrennte CryptoKey-Modus verschlüsselt ausdrücklich ausgewählte Dateien bereits im Browser mit AES-256-GCM. Der Server speichert ausschließlich den versionierten SCK1-Ciphertext und kein wiederherstellbares Schlüsselmaterial; ohne lokale Schlüsseldatei sind Vorschau, OCR, Konvertierung, Signatur und serverseitige Weiterleitung unmöglich.

8. OCR, automatische Dokumentenanalyse und Verfahrenslinien

Sentinel kann Dokumente technisch analysieren und unter anderem:

- Text extrahieren
- Dokumenttypen erkennen beziehungsweise vorschlagen

- Datumsangaben erfassen
- Aktenzeichen erkennen
- Absender und Empfänger strukturieren
- Dokumentzusammenhänge ermitteln
- Dokumente Vorgängen beziehungsweise Verfahrenslinien zuordnen

Beim Virtuellen Bürger-Schreibtisch beginnt die Verfahrensstruktur bereits mit den eingehenden beziehungsweise hochgeladenen Dokumenten und wird mit weiteren Dokumenten fortgeschrieben.

Technische Extraktionen und durch Benutzer vorgenommene Korrekturen werden konzeptionell voneinander unterschieden.

Automatische Zuordnungen und KI-gestützte Vorschläge ersetzen keine rechtliche Bewertung.

9. Einsatz künstlicher Intelligenz

KI-Funktionen werden gegenüber regelbasierten, deterministischen und lokalen Verarbeitungsschritten getrennt betrachtet.

Für Bürgerkonten ist die KI-Nutzung nach der vorliegenden Produktdokumentation standardmäßig deaktiviert und kontospezifisch freizugeben.

Soweit externe KI-Dienste eingesetzt werden, sind Datenkategorien, Zweck, Empfänger, Rechtsgrundlage, Speicherbedingungen und gegebenenfalls Drittlandbezug gesondert zu dokumentieren.

Für bestimmte Recherchefunktionen des Bürger-Schreibtischs ist bereits ein datensparsamer Vertrag vorgesehen, bei dem insbesondere Bürgerdokumente, Aktenzeichen, Notizen sowie Konto- und Vorgangskennungen nicht an den Recherche-Executor übermittelt werden.

KI-Ergebnisse können als ungeprüfte Vorschläge behandelt werden und bedürfen bei entsprechend sensiblen Funktionen einer menschlichen Prüfung.

Status: ZU VERIFIZIEREN: vollständige Liste produktiver externer KI-Datenflüsse

10. Kryptoagilität und Post-Quanten-Vorbereitung

Sentinel Communication besitzt einen versionierten Kryptoagilitätskern mit ML-KEM-768, ML-DSA-65 und AES-256-GCM.

KEM-Roundtrip, Signaturprüfung, AAD-Bindung und Manipulationsablehnung werden durch einen Laufzeit-Selbsttest geprüft.

Ein accountgebundener Schlüsselstore hält versionierte KEM- und Signaturschlüssel. Private Schlüssel werden verschlüsselt gespeichert; Rotation erhält ältere Versionen ausschließlich zur Entschlüsselung bestehender Envelopes. Cross-Account-Zugriff und Manipulation werden in fokussierten Tests abgewiesen.

Fuer den klassischen eBO-Pfad wird das SAFE-Recipient-Cert vor jedem Send auf Gueltigkeit, CA-Status, RSA-Schluesselstaerke und Key Encipherment geprueft. Der erwartete SHA-256-Fingerprint wird in der Java-/Governikus-Engine gegen das tatsaechlich geladene Zertifikat gebunden; Transportverschluesselung ist erzwungen.

Die OSCI-Transportverschluesselung verhindert nicht, dass Sentinel Communication Nachricht und Anlagen vor der Governikus-Uebergabe im Klartext verarbeitet. Der Browser-CryptoKey-Modus ohne Serverklartext ist davon getrennt.

Das aktive Profil bleibt classical-only. SAFE liefert fuer die getesteten Empfaenger keinen verifizierten ML-KEM-Key; der Status provider_validated_not_routed bedeutet, dass Provider, Envelope, Schlüssellebenszyklus und Software-Switch technisch vorhanden sind, eBO-, Dokument- und TLS-Pfade aber noch nicht produktiv auf PQC umgestellt wurden.

Produktive Accountschlüssel werden erst im Rahmen eines freigegebenen Pilotpfads erzeugt. Eine produktive Aktivierung setzt kompatible Gegenstellen, versionierte Transportformate und eine Ende-zu-Ende-Abnahme voraus.

Status: PQC-PROVIDER UND ENVELOPE GETESTET / produktive Kanalintegration offen

11. Protokollierung und Nachvollziehbarkeit

Sicherheits- und fachlich relevante Ereignisse werden abhängig vom jeweiligen Dienst protokolliert. Hierzu können insbesondere gehören:

- Anmeldungen
- fehlgeschlagene Authentisierungsversuche
- Passkey-Registrierungen und -Widerrufe
- Recovery-Vorgänge
- Rollenänderungen
- Freigaben und Widerrufe
- administrative Änderungen
- sicherheitsrelevante Kommunikationsvorgänge
- externe Versandvorgänge

Protokolle sollen dem Nachweis sicherheitsrelevanter Vorgänge dienen, ohne unnötige Inhaltsdaten in zentrale Logsysteme zu übertragen.

Zentrale Betriebs- und Administrationsoberflächen sollen deshalb soweit möglich Status- und Metadaten verarbeiten und nicht automatisch fremde Dokumentinhalte zugänglich machen.

12. Datensparsamkeit und Zweckbindung

Sentinel-Dienste sollen nur die für den jeweiligen Vorgang erforderlichen Daten verarbeiten.

Besonders deutlich wird dieses Prinzip beim Bürger-Schreibtisch und der Schuldnerberatung:

- Ein Bürger gibt nicht automatisch seinen gesamten Schreibtisch an eine Beratungsstelle frei.
- Freigaben können auf einen konkreten Vorgang, eine konkrete Einrichtung beziehungsweise berechtigte Person und definierte Rechte beschränkt werden.
- Private Bürgernotizen werden nicht Bestandteil einer Beratungsfreigabe.
- Ein Widerruf soll den weiteren Zugriff unmittelbar unterbinden.

13. Datensicherung und Wiederherstellung

Die Hetzner-Serverbackups sichern die Systemplatte in sieben Generationen, schließen angehängte Cloud Volumes jedoch ausdrücklich aus.

Produkt- und Bürgerdaten werden deshalb zusätzlich täglich um 12:10 Uhr Europe/Berlin in ein separates 50-GB-Hetzner-Volume gesichert.

Borg verschlüsselt die Archive clientseitig mit repokey-blake2. Videos, laufende Logs und reproduzierbare Caches sind ausgeschlossen.

Portal-JSON-Stores werden in einem kurz angehaltenen Zustand kopiert; SQLite-Stores werden über die SQLite-Backup-API gesichert und vor Archivierung auf Integrität geprüft.

Die Retention umfasst sieben tägliche, vier wöchentliche und sechs monatliche Archive.

Ein vollständiger borg check --verify-data sowie die Testextraktion von 25 JSON-Stores und drei SQLite-Snapshots wurden am 09.10.2026 erfolgreich durchgeführt.

- tägliches verschlüsseltes Borg-Backup
- wöchentlicher vollständiger Datencheck
- wöchentlicher automatisierter Restore-Test
- restriktive Schlüsseldateirechte
- dokumentierter Einzeldatei-, Volume- und Server-Recoverypfad

Status: TECHNISCH VERIFIZIERT AM 09.10.2026; zusätzliche immutable/offsite Kopie bleibt empfohlen

14. Verfügbarkeit und Wiederanlauf

Containerisierte Dienste und persistente Speicherbereiche sind so voneinander getrennt, dass ein Neustart beziehungsweise Austausch eines Anwendungscontainers nicht automatisch zum Verlust persistenter Fachdaten führt.

Für sicherheitskritische Änderungen und Wiederherstellungen werden technische Sicherungen beziehungsweise Snapshots verwendet.

Die Wiederaufnahme des Betriebs nach Störungen erfolgt kontrolliert.

Produktspezifische Anforderungen an Recovery Point Objective (RPO) und Recovery Time Objective (RTO) werden noch gesondert festgelegt.

15. Änderungs- und Patchmanagement

Sentinel unterscheidet Entwicklungs-, Test- beziehungsweise Releaseprozesse und produktive Bereitstellung.

Für Produktinstanzen können unterschiedliche Releasekanäle verwendet werden.

Sicherheitsrelevante Änderungen müssen vor einer produktiven Freigabe angemessen getestet werden.

Bei automatisierter Bereitstellung und zentraler Updateverteilung sind Authentizität, Berechtigung und Nachvollziehbarkeit der Updates sicherzustellen.

Status: ZU VERIFIZIEREN: verbindliche Fristen für kritische Sicherheitsupdates und Umgang mit kundenseitig deaktivierten automatischen Updates

16. Automatisierte Sicherheits- und Regressionstests

Für einzelne Sentinel-Produkte bestehen automatisierte Regressionstests.

Für den Virtuellen Bürger-Schreibtisch dokumentiert der aktuelle Entwicklungsstand insgesamt 397 erfolgreiche Checks.

Hierbei werden unter anderem geprüft:

- Trennung mehrerer Konten
- IDOR-Schutz
- Host-Isolation
- CSRF-Schutz
- Konto- und Mitgliedereinladungen

- Gruppen- und Vorgangsfreigaben
- Rollenwechsel
- Kontosperren
- Sitzungswiderruf
- Passkey-Widerruf
- Recovery
- private Notizen
- Dateizugriffe
- CryptoKey-Container und clientseitig verschlüsselte Downloads
- Pilotberechtigungen
- Schuldnerberatungszugriffe
- sofortiger Freigabewiderruf
- eBO-/Zertifikatsprozesse

Diese Tests stellen technische Regressionstests dar und werden nicht als externe Zertifizierung, Penetrationstest oder unabhängiges Sicherheitsaudit bezeichnet.

Status: TECHNISCHE REGRESSIONSTESTS / keine externe Zertifizierung

17. Datenschutz durch Technikgestaltung

Neue Funktionen sollen bereits während ihrer Entwicklung hinsichtlich Kontentrennung, Berechtigungen und Datenminimierung betrachtet werden. Beispiele hierfür sind:

- unveränderliche Kontozuordnung von Fachobjekten
- standardmäßig fehlende Freigabe fremder Inhalte
- explizite Bürgerfreigaben
- begrenzte Beraterrechte
- getrennte private Notizen
- KI standardmäßig deaktiviert
- kontrollierte Dokumentenübergaben
- serverseitige Berechtigungsprüfung statt reiner UI-Sperren

Damit werden Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen berücksichtigt.

18. Sicherheitsvorfälle

Sicherheitsrelevante Ereignisse werden technisch untersucht und dokumentiert.

Das Verfahren muss mindestens vorsehen:

- Erkennung
- Eindämmung
- Sicherung relevanter Informationen
- Bewertung betroffener Systeme und Daten

- Wiederherstellung
- Dokumentation
- Prüfung gegebenenfalls erforderlicher Meldungen und Benachrichtigungen nach Art. 33 und 34 DSGVO

Status: ZU ERGÄNZEN: verbindliche interne Meldewege, Verantwortlichkeiten und Reaktionsfristen

19. Unterauftragnehmer

Externe Anbieter, die im Rahmen einer Auftragsverarbeitung personenbezogene Daten verarbeiten können, werden in einer gesonderten Unterauftragnehmerübersicht dokumentiert.

Für jeden relevanten Anbieter sind insbesondere festzuhalten:

- Anbieter
- Leistung
- Datenkategorien
- Verarbeitungsort
- Rechtsgrundlage der Einbindung / AV-Vertrag
- gegebenenfalls Drittlandtransfer

Hetzner wird aufgrund des Infrastrukturhostings Bestandteil dieser Übersicht.

Weitere Anbieter werden erst nach Prüfung der tatsächlichen produktiven Datenflüsse aufgenommen.

20. Löschung und Vertragsende

Personenbezogene Daten werden nicht unbegrenzt allein aufgrund ihrer technischen Verfügbarkeit gespeichert.

Produktspezifische Löschfristen berücksichtigen:

- Vertragsverhältnis
- Benutzerkonten
- Dokumente
- Kommunikationsdaten
- Sicherheitsprotokolle
- Backups
- Abrechnungsunterlagen
- gesetzliche Aufbewahrungspflichten

Nach Beendigung einer Auftragsverarbeitung erfolgt die Rückgabe beziehungsweise Löschung nach den vereinbarten Vorgaben, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Status: ZU VERIFIZIEREN: konkrete Fristen je Datenkategorie

21. Regelmäßige Überprüfung

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig sowie anlassbezogen überprüft.

Anlässe sind insbesondere:

- wesentliche Architekturänderungen

- neue externe Dienste
- neue Datenkategorien
- Sicherheitsvorfälle
- Änderungen von Authentisierungs- oder Verschlüsselungsverfahren
- Einführung neuer Kommunikationswege
- erhebliche Produktupdates

Automatisierte Regressionstests ergänzen diese organisatorische Überprüfung.

22. Produktspezifische Anlagen

Die zentralen TOMs werden insbesondere ergänzt durch:

- Anlage TOM-BS: Virtueller Bürger-Schreibtisch
- Anlage TOM-SB: Schuldnerberatung und Beratungsfreigaben
- Anlage TOM-PV: Sentinel Prozessverwaltung
- Anlage TOM-COM: Sentinel Communication / eBO / EGVP
- Anlage KI: KI-Dienste und Datenflüsse
- Anlage SUB: Unterauftragnehmer
- Anlage LÖ: Lösch- und Aufbewahrungskonzept
- Anlage IR: Incident-Response- und Wiederherstellungskonzept

23. Versionsführung

Die TOMs werden versioniert geführt. Wesentliche Änderungen an Sicherheitsmaßnahmen, Datenflüssen oder eingesetzten Unterauftragnehmern werden dokumentiert und in den jeweils einschlägigen Vertragsverhältnissen berücksichtigt.