Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO — Anhang III zur Vereinbarung über die Auftragsverarbeitung (AVV) · Floriti

Stand: 23. Oktober 2026 · Anbieter: Tasker & Fox GmbH, Hohenlohestraße 17, 80637 München. Dieses Dokument beschreibt den tatsächlich implementierten Stand der technischen und organisatorischen Maßnahmen der Floriti-Plattform.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle (physisch)

Der Betrieb der Plattform erfolgt ausschließlich in Rechenzentren der Hetzner Online GmbH in Falkenstein (Deutschland). Die Rechenzentren sind nach ISO/IEC 27001 zertifiziert; der physische Zutritt ist durch Zutrittskontrollsysteme, Videoüberwachung und Sicherheitspersonal des Rechenzentrumsbetreibers geschützt. Verschlüsselte Sicherungskopien werden zusätzlich in Rechenzentren der Hetzner Online GmbH in Helsinki (Finnland) und der Scaleway SAS in Paris (Frankreich) gespeichert; diese Anbieter erhalten ausschließlich verschlüsselte Daten (siehe Ziffer 3). Der Anbieter selbst unterhält keine eigenen Serverräume.

1.2 Zugangskontrolle (Systeme)

- Administrativer Serverzugriff ausschließlich über verschlüsselte SSH-Verbindungen; Zugriff nur durch den Anbieter.
- Anwendungszugang nur mit persönlichem Benutzerkonto; Passwörter werden ausschließlich als gesalzene Hashes (bcrypt) gespeichert.
- Optionale Anbindung an das Identitätsmanagement des Kunden per Single Sign-on (OpenID Connect).
- Sitzungen über signierte Tokens (JWT) mit instanz-eigenem Geheimschlüssel; jede Kundeninstanz besitzt eigene kryptografische Schlüssel.

1.3 Zugriffskontrolle (Daten)

- Rollenbasiertes Berechtigungskonzept (Administrator, Bearbeiter, Genehmiger, Leser, Direktbearbeiter) mit Benutzergruppen.
- Berechtigungen wirken bis auf Register- und Funktionsebene; Benutzer sehen nur die ihnen zugewiesenen Inhalte.
- Der Reporting-Datenbankzugang ist ein separater Nur-Lese-Benutzer und durch eine vom Kunden selbst verwaltete IP-Freigabeliste geschützt (Standard: geschlossen).

1.4 Trennungskontrolle

- Mandantentrennung durch Architektur: Jeder Kunde erhält eine eigene Anwendungsinstanz und eine eigene PostgreSQL-Datenbank (keine geteilten Tabellen, keine mandantenübergreifenden Abfragen).
- Instanzen laufen in getrennten Container-Umgebungen mit eigenen Netzwerken, Zugangsdaten und Schlüsseln.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Übertragungskontrolle

- Sämtliche Verbindungen zur Anwendung sind TLS-verschlüsselt (HTTPS); Zertifikate werden automatisiert ausgestellt und erneuert (Let's Encrypt).
- Auch der direkte Reporting-Datenbankzugriff erfolgt TLS-verschlüsselt.
- Unverschlüsselte HTTP-Aufrufe werden serverseitig auf HTTPS umgeleitet.

2.2 Eingabekontrolle

- Lückenloses Aktivitätsprotokoll: Jede Änderung wird mit Benutzer, Zeitpunkt und geänderten Feldern protokolliert (Bearbeitungshistorie pro Feld).
- Optionale Genehmigungs-Workflows setzen ein Vier-Augen-Prinzip durch (Entwurf → Prüfung → Genehmigung) mit nachvollziehbarer Historie.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Tägliche automatisierte Sicherung aller Kundendatenbanken (pg_dump, komprimiert) mit 14 Tagen Aufbewahrung sowie tägliche Sicherung der Instanz-Konfiguration.
- Zusätzlich wird jede Nacht ein Sicherungspaket (alle Instanz-Datenbanken, Datei-Anhänge und Instanz-Konfiguration) auf dem Server mit einem asymmetrischen öffentlichen Schlüssel (age) verschlüsselt. Der Server kann nur verschlüsseln, nicht entschlüsseln; der private Schlüssel wird offline bei der Geschäftsführung verwahrt (Passwort-Manager und Papier). Die Speicheranbieter erhalten ausschließlich verschlüsselte Daten.
- Das verschlüsselte Sicherungspaket wird an zwei voneinander unabhängigen Standorten bei zwei verschiedenen Anbietern in der EU abgelegt: Hetzner Storage Box (Hetzner Online GmbH, Rechenzentrum Helsinki, Finnland) und Scaleway Object Storage (Scaleway SAS, Region Paris, Frankreich).
- Löschschutz: Die Storage Box ist durch Snapshots geschützt, die der Produktionsserver nicht verwalten kann. Im Object Storage verhindert eine Objektsperre (Object Lock), dass Sicherungen innerhalb von 12 Tagen gelöscht oder verändert werden – auch nicht durch den Anbieter selbst. Die Aufbewahrung beträgt an beiden Standorten 14 Tage; ältere Sicherungen werden automatisch gelöscht.
- Überwachung: Schlägt eine Sicherung fehl oder bleibt sie aus, wird der Anbieter automatisch per E-Mail alarmiert. Wöchentlich wird automatisch ein Datenbank-Dump testweise in eine Wegwerf-Datenbank wiederhergestellt.
- Wiederherstellung einzelner Instanzen aus der Sicherung auf Anfrage im Rahmen des Supports.
- Automatischer Neustart der Dienste bei Störungen (Container-Restart-Richtlinien); Überwachung des Serverzustands.
- Kapazitätsreserven: Ressourcenlimits pro Instanz verhindern, dass eine einzelne Instanz die Plattform beeinträchtigt.

4. KI-Funktionen und Datenabfluss

- KI-Funktionen sind bei Kundeninstanzen (Pakete Starter und Full) standardmäßig deaktiviert und werden nur durch einen Administrator des Kunden freigeschaltet; die Freischaltung wird protokolliert und kann jederzeit widerrufen werden.
- Die KI-Wissensbasis (semantische Indexierung hochgeladener Dokumente) wird vollständig auf eigenen Servern des Anbieters in Deutschland verarbeitet (selbst gehostetes Embedding-Modell); eine Übermittlung der Dokumente an Dritt-KI-Dienste findet hierfür nicht statt.
- Nur bei aktivierter KI-Analyse werden die zur Analyse übermittelten Texte per API durch den vom Kunden gewählten KI-Anbieter verarbeitet: Anthropic PBC (USA, auf Grundlage der EU-Standardvertragsklauseln) oder Mistral AI SAS (Frankreich, EU). Die Wahl erfolgt je Instanz und kann je Register abweichend festgelegt werden; sie wird protokolliert. Steht der gewählte Anbieter nicht

zur Verfügung, weicht die Plattform technisch nicht auf einen anderen Anbieter aus. Anthropic verwendet API-Daten standardmäßig nicht zum Training von Modellen.

5. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Regelmäßige Einspielung von Sicherheitsaktualisierungen (Betriebssystem, Container-Images, Abhängigkeiten).
- Protokollierte Provisionierungs- und Löschprozesse; fehlgeschlagene Vorgänge werden automatisch zurückgerollt und gemeldet.
- Externe Penetrationstests sind Bestandteil der Sicherheits-Roadmap.

6. Auftragskontrolle / Unterauftragsverarbeiter

Es werden ausschließlich die folgenden Unterauftragsverarbeiter eingesetzt; mit allen bestehen Auftragsverarbeitungsverträge bzw. Standardvertragsklauseln (Einzelheiten siehe Anhang IV der AVV):

Unterauftragsverarbeiter	Zweck	Standort
Hetzner Online GmbH	Hosting, Server-Infrastruktur, Rechenzentrum; Speicherung verschlüsselter Sicherungskopien (Storage Box)	Deutschland (Falkenstein/Sachsen); Sicherungskopien: Finnland (Helsinki)
Scaleway SAS	Speicherung verschlüsselter Sicherungskopien (Object Storage); kein Zugriff auf den Schlüssel	EU (Frankreich, Region Paris)
Heinlein Hosting GmbH (mailbox.org)	E-Mail-Postfächer des Anbieters (Support- und Kontaktkommunikation)	Deutschland (Berlin)
Sendinblue SAS (Brevo)	Versand von Transaktions-E-Mails	EU (Frankreich)
Anthropic PBC	KI-Analyse — NUR bei ausdrücklicher Freischaltung und Wahl durch den Verantwortlichen	USA (EU-Standardvertragsklauseln 2021/914, Modul 3)
Mistral AI SAS	KI-Analyse — NUR bei ausdrücklicher Freischaltung und Wahl durch den Verantwortlichen	EU (Frankreich); etwaige Übermittlungen durch Unter-Dienstleister gemäß Mistral-DPA (Angemessenheitsbeschluss bzw. Standardvertragsklauseln)

7. Löschung und Datenportabilität

- Vollständiger Datenexport (Excel/CSV/ZIP inklusive Datei-Anhängen) jederzeit durch den Kunden selbst möglich — kein Anbieter-Lock-in.
- Bei Vertragsende werden Instanz, Datenbank und Datei-Anhänge auf Wunsch vollständig und endgültig gelöscht; Sicherungskopien rotieren binnen 14 Tagen automatisch aus.