Technical and Organisational Measures (TOM)

pursuant to Art. 32 GDPR — Annex III to the Data Processing Agreement (DPA) · Floriti

As of: 23 October 2026 · Provider: Tasker & Fox GmbH, Hohenlohestraße 17, 80637 München. This document describes the technical and organisational measures of the Floriti platform as actually implemented. This is a convenience translation – only the German version is legally binding.

1. Confidentiality (Art. 32(1)(b) GDPR)

1.1 Physical access control

Operation of the platform takes place exclusively in data centres of Hetzner Online GmbH in Falkenstein (Germany). The data centres are certified in accordance with ISO/IEC 27001; physical access is protected by access control systems, video surveillance and security personnel of the data centre operator. Encrypted backup copies are additionally stored in data centres of Hetzner Online GmbH in Helsinki (Finland) and of Scaleway SAS in Paris (France); these providers receive encrypted data only (see section 3). The Provider itself does not maintain any server rooms of its own.

1.2 System access control

- Administrative server access exclusively via encrypted SSH connections; access by the Provider only.
- Application access only with a personal user account; passwords are stored exclusively as salted hashes (bcrypt).
- Optional connection to the Customer's identity management via single sign-on (OpenID Connect).
- Sessions via signed tokens (JWT) with an instance-specific secret key; each Customer instance has its own cryptographic keys.

1.3 Data access control

- Role-based authorisation concept (administrator, editor, approver, reader, direct editor) with user groups.
- Permissions take effect down to register and function level; users only see the content assigned to them.
- The reporting database access is a separate read-only user and is protected by an IP allowlist managed by the Customer itself (default: closed).

1.4 Separation control

- Tenant separation by architecture: each Customer receives its own application instance and its own PostgreSQL database (no shared tables, no cross-tenant queries).
- Instances run in separate container environments with their own networks, credentials and keys.

2. Integrity (Art. 32(1)(b) GDPR)

2.1 Transfer control

- All connections to the application are TLS-encrypted (HTTPS); certificates are issued and renewed automatically (Let's Encrypt).
- Direct reporting database access is also TLS-encrypted.
- Unencrypted HTTP requests are redirected to HTTPS on the server side.

2.2 Input control

- Complete activity log: every change is logged with the user, time and changed fields (editing history per field).
- Optional approval workflows enforce a four-eyes principle (draft → review → approval) with a traceable history.

3. Availability and resilience (Art. 32(1)(b) and (c) GDPR)

- Daily automated backup of all Customer databases (pg_dump, compressed) with 14-day retention, as well as daily backup of the instance configuration.
- In addition, every night one backup bundle (all instance databases, file attachments and instance configuration) is encrypted on the server with an asymmetric public key (age). The server can only encrypt, not decrypt; the private key is kept offline by the management (password manager and paper). The storage providers receive encrypted data only.
- The encrypted backup bundle is stored at two mutually independent locations with two different providers in the EU: Hetzner Storage Box (Hetzner Online GmbH, data centre Helsinki, Finland) and Scaleway Object Storage (Scaleway SAS, Paris region, France).
- Deletion protection: the Storage Box is protected by snapshots that the production server cannot manage. In the Object Storage, an object lock prevents backups from being deleted or altered for 12 days – not even by the Provider itself. Retention at both locations is 14 days; older backups are deleted automatically.
- Monitoring: if a backup fails or is missing, the Provider is automatically alerted by e-mail. Every week, a database dump is automatically test-restored into a throw-away database.
- Restoration of individual instances from the backup upon request as part of the support.
- Automatic restart of services in the event of malfunctions (container restart policies); monitoring of server health.
- Capacity reserves: resource limits per instance prevent a single instance from impairing the platform.

4. AI functions and data outflow

- AI functions are deactivated by default for Customer instances (Starter and Full plans) and are only enabled by an administrator of the Customer; enablement is logged and can be revoked at any time.
- The AI knowledge base (semantic indexing of uploaded documents) is processed entirely on the Provider's own servers in Germany (self-hosted embedding model); no transfer of the documents to third-party AI services takes place for this purpose.
- Only if AI analysis is activated are the texts submitted for analysis processed via API by the AI provider selected by the Customer: Anthropic PBC (USA, on the basis of the EU Standard Contractual Clauses) or Mistral AI SAS (France, EU). The selection is made per instance and may differ per register; it is logged. If the selected provider is unavailable, the platform does not technically fall back to another provider. By default, Anthropic does not use API data to train models.

5. Procedures for regular review (Art. 32(1)(d) GDPR)

- Regular installation of security updates (operating system, container images, dependencies).
- Logged provisioning and deletion processes; failed operations are automatically rolled back and reported.
- External penetration tests are part of the security roadmap.

6. Order control / sub-processors

Only the following sub-processors are used; data processing agreements or Standard Contractual Clauses are in place with all of them (for details, see Annex IV to the DPA):

Sub-processor	Purpose	Location
Hetzner Online GmbH	Hosting, server infrastructure, data centre; storage of encrypted backup copies (Storage Box)	Germany (Falkenstein/Saxony); backup copies: Finland (Helsinki)
Scaleway SAS	Storage of encrypted backup copies (Object Storage); no access to the key	EU (France, Paris region)
Heinlein Hosting GmbH (mailbox.org)	The Provider's e-mail mailboxes (support and contact communication)	Germany (Berlin)
Sendinblue SAS (Brevo)	Sending of transactional e-mails	EU (France)
Anthropic PBC	AI analysis — ONLY if expressly enabled and selected by the controller	USA (EU Standard Contractual Clauses 2021/914, Module 3)
Mistral AI SAS	AI analysis — ONLY if expressly enabled and selected by the controller	EU (France); any transfers by its own sub-processors in accordance with Mistral AI's DPA (adequacy decision or standard contractual clauses)

7. Deletion and data portability

- Complete data export (Excel/CSV/ZIP including file attachments) possible at any time by the Customer itself — no vendor lock-in.
- Upon termination of the contract, the instance, database and file attachments are completely and permanently deleted upon request; backup copies are automatically rotated out within 14 days.