

Technical and Organisational Measures

Annex 1 to the Data Processing Agreement of Founders1 GmbH

As of: October 2026 · Version 2026-1 · supersedes the version of June 2024 · Convenience translation – the German version is binding

Preliminary remarks

This Annex describes the technical and organisational measures under Art. 32 GDPR that Founders1 GmbH (Contractor) takes when processing personal data on behalf of its customers (Clients). It forms part of the Data Processing Agreement.

The Contractor is a distributed, mobile-working company. It does not maintain its own office or server premises and operates paperlessly. The platform is operated exclusively on the Microsoft Azure cloud infrastructure, region Germany West Central (Frankfurt am Main).

Some of the measures, in particular the physical security of the data centres, are provided by the cloud provider Microsoft Ireland Operations Ltd. These measures are marked as such in each case; evidence is provided through Microsoft's certifications and documentation, including under ISO/IEC 27001.

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

1.1 Physical access control

The Contractor does not maintain its own office or server premises. Physical access control to the data centres is provided by Microsoft:

- Access only after authentication with a personal access card
- Visitors only with prior registration and permanent escort, without access to secured areas
- 24/7 security guards, alarm system, airlock system, video surveillance and logging of entries
- Locked server racks

1.2 System access control

- All systems and applications are accessible only after authentication.
- Personal user accounts for each individual; group accounts are not permitted, including for administrative access.
- Multi-factor authentication for production environments, administrative access, the cloud portal, source code management, key vaults and e-mail.
- Passwords of at least 12 characters combined with mandatory multi-factor authentication; initial passwords for one-time use only.
- Automatic screen lock after no more than 15 minutes.
- Immediate blocking of accounts and sessions when a person leaves or a device is lost.

End devices. Employees work on their own end devices. The following applies:

- Client Matter Data is not stored locally on end devices; processing takes place exclusively server-side.
- Access takes place exclusively via encrypted connections.
- Employees undertake in text form to comply with device requirements, in particular hard-disk encryption and screen lock.
- On leaving, they confirm in text form that all company data has been removed.

1.3 Data access control

- Role-based authorisation concept; permissions granted exclusively on a need-to-know basis.
- Differentiated rights in applications and the database; database rights limited to what is necessary.
- Minimum number of administrative accounts.
- Logging of input, modification and deletion in the application.
- Review of permissions at least annually, and every six months for production and administrative access, in each case documented.
- Encryption of stored data: file storage in Azure with platform-managed keys, database at MongoDB Atlas with provider-managed keys.
- Access by cloud provider personnel: Customer Lockbox for Microsoft Azure is enabled, and support access to the MongoDB Atlas backend infrastructure is blocked. Approval is granted only by the Contractor on a case-by-case basis, in critical incidents affecting operations or security, for a limited period and logged.

1.4 Separation control

- Separate development, test and production environments.
- Multi-tenant application with separation of data per Client.
- Documents are stored in a separate storage area per record; no storage area is publicly accessible.
- Development and test environments use exclusively generated test data, never personal data from production.

1.5 Pseudonymisation

The purpose of processing is the identification of individuals and companies under the GwG (German Anti-Money Laundering Act); this requires that data can be attributed. Pseudonymisation is used where the purpose permits. In that case, attribution data is kept separately and encrypted.

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

2.1 Transfer control

- Connections between Users and the platform are encrypted with TLS 1.2 or 1.3; unencrypted requests are redirected to HTTPS.
- No disclosure to third parties beyond contractual obligations.
- Client Matter Data is not transferred into e-mail, chat or ticketing systems; support is provided without transmitting client matter content.
- Sub-processors engaged exclusively in accordance with Annex 2, in each case under a contract pursuant to Art. 28 GDPR.
- Storage and processing of Client Matter Data in the European Economic Area; Annex 2 states the locations for each service. Support access by cloud providers only in accordance with clause 1.3 and clause 6.2 DPA.

2.2 Input control

- Traceability of input, modification and deletion via personal user accounts.
- Rights to input, modify and delete in accordance with the authorisation concept.
- Clear responsibilities for deletions and their logging.
- Sample-based and event-driven evaluation of logs.
- Logs contain no client matter content and no personal data beyond what is necessary to attribute actors and actions.

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

- Four-tier backup concept: hourly (retention 2 days), daily (7 days), weekly (4 weeks) and monthly (12 months).
- Backups are encrypted and remain in the European Economic Area.
- Disaster recovery takes place exclusively in Azure regions within the European Economic Area.
- Access to backups is separate from access to the production environment.
- Monitoring of backup runs; a failed run is treated as an incident.
- Targets: recovery point objective (RPO) 6 hours; recovery time objective (RTO) 8 hours for infrastructure and database, 12 hours for applications.
- Restore tests at least annually, documented.

Provided by Microsoft: fire detection and suppression systems, air conditioning, uninterruptible power supply, redundant storage systems, flood protection and monitoring and alarms for the server rooms.

4 Regular testing, assessment and evaluation (Art. 32(1)(d), Art. 25 GDPR)

- Central documentation of all rules on data protection and information security.
- Annual review of these measures and the underlying policies, documented.
- Data protection training for employees on joining and at regular intervals.
- Procedure for detecting, assessing, documenting and following up on security incidents.
- Notification of a personal data breach to the Client without undue delay, at the latest within 48 hours of becoming aware of it.
- Support for the Client with data subject requests and data protection impact assessments.
- Data protection by default: only the data necessary for the respective purpose is processed.
- Careful selection and ongoing monitoring of sub-processors.

Evidence. The Contractor currently holds no certification of its own. Evidence is provided by this Annex, the result of the annual effectiveness review, the Client's contractual audit rights and the sub-processors' certifications.

5 Processing using artificial intelligence

The platform uses a language model to read uploaded documents and pre-fill information.

- **Processing route.** Exclusively Azure OpenAI Service of Microsoft Ireland Operations Ltd, in a deployment restricted to the EU Data Zone; the resource is located in the Germany West Central region. Microsoft does not use inputs or outputs to train models. No other AI services are used.
- **Isolation and data minimisation.** For each call, the model receives only the relevant document. It has no access to databases, credentials or other systems and retains nothing between calls. Instructions contained in documents are treated as content; results are checked for manipulation attempts.
- **Structured results.** The model returns only predefined fields with source references (page and text passage). Other values are discarded.
- **Proposal, not decision.** AI values are marked as such and are adopted only after confirmation or correction by a human. Existing information is not overwritten without confirmation. The AI does not assess individuals, assign risk ratings or make decisions within the meaning of Art. 22 GDPR.
- **Health data.** Medical documents are recognised and filed as such; their content is neither evaluated nor adopted.

- **Traceability.** For each value, the source document, page, confidence, status and the confirming person and date are stored. Logs contain no document content.
- **Outage.** If the service is unavailable, the documents remain stored; the information is entered manually.
- **Quality assurance.** Before any model change, the model is tested against a fixed set of fictitious sample documents with known target values and is deployed only once it has passed the test.

6 Professional secrecy

For Clients who are professional secrecy holders, § 203 StGB (German Criminal Code) applies in addition to data protection law. The Professional Secrecy Agreement applies supplementarily.

- All persons with access to Client Matter Data are bound to confidentiality in text form before commencing their activities, including information on criminal liability.
- Corresponding obligation of sub-processors that receive Client Matter Data, including the obligation of their own subcontractors. Microsoft and MongoDB do not offer a separate undertaking under § 203 StGB; access by their personnel is blocked in accordance with clause 1.3 and possible only following approval.
- Maintenance of a register of undertakings, the current status of which is disclosed to the Client on request.

7 Changes

The Contractor continues to develop the measures. The level of protection set out in this Annex will not be reduced. Material changes are notified to the Client in advance in text form.

Founders1 GmbH · Registered office Berlin, Amtsgericht Charlottenburg, HRB 234373 B ·
Business address Berger Straße 224, 60385 Frankfurt am Main