

Technical and Organizational Measures acc. to Art. 32 GDPR

Version date: October 26th, 2026

Provider: Aam Digital GmbH

c/o Impact Hub Berlin, Rollbergstraße 28 A, 12053 Berlin, Germany

Registered at Amtsgericht Charlottenburg Berlin: HRB 228183

info@aam-digital.com

aam-digital.com

Scope and Interpretation

These Technical and Organizational Measures (TOMs) apply to hosted software services and customer environments operated by Aam Digital GmbH ("Provider") and, for self-hosted services, only to the extent Provider processes personal data on behalf of a Customer and controls the relevant processing systems.

For purposes of these TOMs, "Customer" means the relevant customer or contracting party; "Applicable Agreement" means the contract or contractual documents governing the relevant services between Provider and Customer; "Applicable DPA" means the data processing agreement applicable to the relevant customer relationship; "Customer Data" means personal data processed by Provider on behalf of Customer under the Applicable DPA; "Authorized User" means an individual authorized by Customer to access the relevant Hosted Service; and "Hosted Service" means a hosted Aam Digital software service or customer environment operated by Provider for Customer. "Standard Subprocessor List" means Provider's current List of Standard Subprocessors available at <https://www.aam-digital.com/legal/subprocessors>; "Standard Subprocessor" means a subprocessor identified in that list. Where the Applicable Agreement or Applicable DPA uses different terminology, the corresponding contractual terminology applies.

These TOMs describe technical and organizational security measures under Art. 32 GDPR. They do not create service levels, customer-specific commitments, or other operational commitments unless such commitments are expressly stated in the Applicable Agreement, the Applicable DPA, a customer-specific TOMs addendum, or another binding document.

Backup, restore, export, retention, deletion, and subprocessor-change rules are governed by the Applicable Agreement and the Applicable DPA.

For purposes of these TOMs, "Provider personnel" means employees, contractors, freelancers, and other natural persons acting under Provider's direct authority who are authorized to perform relevant activities for Provider.

General Measures

- The protection of personal data is considered at all levels of our work, taking into account the state of the art, implementation costs, and the nature, scope, context and purposes of processing, as well as the likelihood and severity of risks to the rights and freedoms of natural persons. We consider these implications during development of software and selection of modules and processes, following the data protection principles of data protection by design and privacy-friendly defaults (Art. 25 GDPR). There is an in-house data protection management system, compliance with which is monitored and evaluated periodically, taking into account relevant risks and changes in processing.

- All Provider personnel are conscious of their responsibilities handling sensitive data and bound to secrecy, security measures and data protection standards in a written data protection undertaking.
- The keys, access cards or codes issued to Provider personnel as well as authorizations granted with regard to the processing of personal data will be withdrawn when they cease providing relevant services to Provider or change responsibilities.
- Data protection training: Provider personnel with relevant responsibilities are trained regularly on data protection and security. In addition to general training, the special context of sensitive data that Customers may process through the Aam Digital software, including data about beneficiaries, participants, clients, or other individuals, and the associated risks and protective measures are addressed as appropriate.
- Security testing and audits: Provider regularly tests, assesses and evaluates security measures for the Aam Digital software, servers and related systems. Appropriate methods may include attack scenario modeling, penetration testing, vulnerability scanning, automated security analysis, code review, and discussion and adaptation of security measures based on the results. Where appropriate, Provider takes into account recognized security guidelines, including those from the German Federal Cyber Security Authority (BSI "IT Grundschutz") and the "Open Web Application Security Project" (OWASP).
- Data minimization guidance: Provider may make standard documentation, guidance or configuration information available to support Customers in applying data minimization principles. Customer remains responsible, in accordance with its role in the relevant processing chain, for ensuring that the data processed through the Hosted Service is necessary, lawful and appropriate for the relevant use case.

Entry Control

- Hosted production environment: The hosted production environment is operated using data-center infrastructure subject to appropriate physical and organizational security controls. Provider's standard service model is to host Customer Data and operate the Hosted Service production environment exclusively within the EU/EEA using hosting infrastructure covered by ISO/IEC 27001 certification, unless expressly agreed or disclosed otherwise in the Applicable Agreement, the Applicable DPA, the Standard Subprocessor List, a customer-specific subprocessor authorization, or another binding document. Provider-controlled processing of Customer Data on Customer's behalf under the Applicable DPA, including processing through Provider personnel, infrastructure, and subprocessors, is also carried out within the EU/EEA unless an exception is expressly agreed or disclosed in those binding documents. Feature-specific processing by an authorized Standard Subprocessor may occur outside the EU/EEA where expressly identified in the Standard Subprocessor List. Such feature-specific processing does not change the hosting location of Customer Data in the production environment unless expressly stated in a binding document. Separate processing for which Provider acts as controller is governed by Provider's applicable privacy notices and may involve processing outside the EU/EEA as disclosed there. The location commitment for processing on Customer's behalf applies to processing locations controlled or selected by Provider and does not restrict Customer- or Authorized User-controlled devices or Customer-directed retrieval, export, API use, email notification, integration, or other transmission to systems, recipients, or destinations selected or controlled by Customer or its Authorized Users. Any customer-specific data residency, Provider-controlled processing-location, remote-access, subprocessor-location, or transfer-related commitment or deviation applies only if

expressly stated in the Applicable Agreement, the Applicable DPA, a customer-specific TOMs addendum, or another binding document and remains subject to technical feasibility, applicable data protection law, the agreed subprocessor authorization mechanism, and any required GDPR transfer safeguards.

- Data centers with strict access control: electronic physical access-control systems with logging; documented distribution and regular review of access media and access rights; high-security perimeter fencing around the data-center parks; comprehensive video monitoring of relevant areas, including entrances, exits, security airlocks and server rooms; documented procedures for registering, authorizing and accompanying external visitors; and data-center technical staff present 24/7.

Access Control

- Server access strictly restricted: Only a few, carefully selected Provider personnel have IT administrator access to servers containing Customer Data for the Hosted Service. They are trained and bound in writing to strict confidentiality and security requirements.
- Administrative access to Provider-controlled servers is restricted to authorized personnel and uses encrypted, strongly authenticated access mechanisms.
- Server firewall: The servers are protected by a firewall and configured securely according to the state of the art.
- Server updates: Servers are promptly updated with any security patches and their status is checked manually on a regular basis.
- Software development quality controls: To prevent security gaps in the Aam Digital development process, tools for automated code analysis, automated software tests, and code reviews by at least one other experienced developer are used.
- Software development with dependency management & updates: Software libraries upon which the Aam Digital software is technically based are regularly updated and automatically checked for critical security updates.
- App with password guidelines: Users access the Aam Digital application through individual accounts and applicable authentication mechanisms, such as passwords, SSO, or additional verification where configured. Where password-based authentication is used, technical password guidelines require passwords to meet minimum length and complexity requirements. Hashed passwords: The Aam Digital application stores passwords as salted cryptographic hashes rather than in plain text, reducing the risk that stored credential data can be directly used if it is accessed without authorization.
- Role-based Access Control: Where available and configured for the relevant customer environment, users can be assigned roles or permissions to limit access to certain subsets of data. Customer remains responsible for configuring user access appropriately.
- Multi-factor / additional verification: Where available and configured for the relevant customer environment, users may be required to log in with two factors or additional verification (e.g. an email code) on new devices to reduce the risk of unauthorized access through stolen passwords.
- API access controls: Where API functionality is available, API access requires dedicated authentication credentials associated with the relevant customer environment. These credentials are separate from individual Authorized User accounts, may be limited, and can be revoked. Data made available through the API is determined by configured reports or

other outputs configured by users with the required configuration permissions, typically administrators; API access does not inherit an individual user account's permissions. API transmissions use encrypted transport.

Usage & Transfer Control

- Transport encryption: Data from the Aam Digital application is only transmitted in encrypted form. The application does not allow insecure connections and automatically redirects to a TLS/SSL encrypted connection.
- Encryption with secure procedures: Outdated, insecure encryption standards are technically not permitted in order to prevent downgrade attacks.
- Encryption at rest for production storage: Customer Data in Provider-controlled production storage is encrypted at rest.
- Encryption of backups: Backups of Customer Data from the Hosted Service are only created in encrypted form.
- Encryption of emails: Communication via e-mail and file attachments can be protected by end-to-end encryption (OpenPGP or S/MIME), provided that the communication partner supports this on their part. Dedicated data transfer authorizations: All Provider personnel are obliged in writing and sensitized through regular training to never share their access with unauthorized persons and to never pass on data.

Order or Contract Control

- Supplier security assessment: Before engaging a subprocessor or another provider that will have access to personal data or security-relevant Provider systems, Provider assesses the provider's security measures in a manner proportionate to the nature of the services and associated risks. The assessment may include, as appropriate, review of certifications such as ISO 27001 or SOC 2, security documentation, contractual security commitments, and other relevant information, and considers appropriate technical and organizational security measures, including, as applicable, encryption in transit, access control, confidentiality, security-incident notification, and other controls appropriate to the services and associated risks. Provider reviews the continued suitability of such providers where their services or risk profile change materially and otherwise periodically based on risk as part of Provider's security and data-protection review processes.
- Controlled processing by subprocessors and other providers: Where subprocessors or other third-party providers are used for processing personal data, they are bound by contractual commitments required under applicable data protection law, including Art. 28 GDPR where applicable. The applicable authorization, information, notice, and objection mechanisms for subprocessors are governed by the Applicable DPA.
- Deletion and retention of data: Deletion, return, retention after termination, and backup lifecycle rules are governed by the Applicable Agreement and the Applicable DPA. Provider deletes or returns personal data in accordance with those documents, Customer's documented instructions where applicable, and applicable law.
- Processing of beneficiary data and data subject requests: Aam Digital may process personal data about beneficiaries or other data subjects on behalf of Customer as processor or subprocessor under the Applicable DPA. Customer, or where applicable the relevant underlying controller, is responsible for the legitimacy of processing and for handling data subject requests in accordance with the applicable role allocation. Provider

supports Customer with reasonable assistance as required by Art. 28(3) GDPR, taking into account the nature of processing, the information available to Provider, and Provider's scope of responsibility. Extraordinary assistance beyond Provider's standard support and compliance processes may be subject to reasonable additional charges agreed with Customer, unless the assistance is required due to Provider's breach of the Applicable DPA or applicable law.

- Handling data only based on documented instructions: As processor, Provider personnel handle Customer Data in the Hosted Service only on Customer's documented instructions, as permitted by the Applicable Agreement and the Applicable DPA, or as required by applicable law. Provider personnel participate in related training and are bound by written confidentiality, security, and data protection undertakings.
- Instructions are documented in writing or text form, including electronic form, or another legally sufficient form.

Availability & Integrity

- Data centers with redundant systems: employment of an uninterruptible power supply system or emergency power supply system; permanently active DDoS protection
- Server and application monitoring: The application and servers are monitored by an automated monitoring system. In the event of system failures, our technicians are automatically alerted. Potential errors in the application are evaluated and regularly checked.
- Automated backups: Customer Data from the Hosted Service is automatically backed up to encrypted files on a daily basis, subject to the applicable backup and related data-continuity rules in the Applicable Agreement and the Applicable DPA. Backups are maintained for security, availability, integrity, resilience, and operational recovery purposes. Backup availability does not by itself create any restore, migration, or disaster-recovery commitment beyond the Applicable Agreement and the Applicable DPA.
- Backup and recovery concept: The concept for backing up and operational recovery is checked regularly. A recovery process is carried out regularly on a trial basis for testing and practice. Such testing supports operational preparedness and does not create restore or disaster-recovery commitments beyond those stated in the Applicable Agreement and the Applicable DPA.
- Offline-first local storage: The hosted application is designed on an offline-first basis by default. This design reflects the operational realities of many organizations using Aam Digital, including work in locations where internet connectivity may be unavailable, intermittent, or unreliable. Offline-first does not mean that users are expected to work offline; users can and ordinarily do use the Hosted Service while connected to the internet. Customer Data may nevertheless be stored locally on Authorized User devices so that relevant work can continue during temporary loss of connectivity and synchronize with the Hosted Service when the relevant user is logged in and connectivity is available. Where available for the relevant customer environment and enabled, an online-only configuration may prevent Customer Data from being stored locally for offline continuity.
- Local device copies and device security: Customer- or Authorized User-controlled devices are outside Provider's physical control. Provider cannot independently access or remotely erase a locally stored copy. In normal use, server-side deletions and other relevant changes are ordinarily reflected in locally stored Customer Data when the relevant Authorized User is logged into the Hosted Service on that device and the application

successfully synchronizes. However, server-side deletion, permission changes, logout, or other account or synchronization changes may not immediately remove or modify data previously stored on a device that has not synchronized. If the relevant Authorized User does not subsequently log back in on that device while access remains available, or synchronization cannot take place, the local copy may remain until it is otherwise removed from the device. Customer remains responsible for appropriate device security and management, including device access controls and device-level encryption where appropriate for Customer's use case and risk profile.

- Logical client separation (software): Instances of the application for each client are run completely separated from each other in a virtualized server environment. This ensures isolation of each client's data from access by other parties.
- Separation of production and test systems.

Subprocessors

The current and authoritative List of Standard Subprocessors used for relevant processing on behalf of Customers is available at <https://www.aam-digital.com/legal/subprocessors>. The list identifies the relevant providers, purposes, categories of data, data subjects, processing locations, and, where applicable, international-transfer safeguards. The authorization, notice, objection, and other contractual rules applicable to subprocessors are governed by the Applicable DPA. Customer-specific subprocessors, where the Applicable DPA provides for them, may be separately authorized in accordance with the Applicable DPA and the relevant customer-specific authorization. This TOMs document therefore does not maintain a separate subprocessor table.