



Technical and Operational Measures acc. to Art. 32 GDPR

Aam Digital GmbH

Data Protection & Security Concept	2
General Measures	2
Entry Control	2
Access Control	3
Usage & Transfer Control	3
Order or Contract Control	4
Availability & Integrity	4

Data Protection & Security Concept

Technical and operational measures acc. to Art. 32 GDPR

General Measures

- The protection of personal data is considered at all levels of our work, taking into account technical state of the art, cost of implementation and type, scope, context and purposes of the data processing as well as the diverse probability and impact of risks for the rights and freedom of affected persons. We already consider these implications during development of software and selection of modules and processes following the data protection principle of designing for data protection and privacy friendly defaults (Art. 25 GDPR). There is an in-house data protection management system, compliance with which is constantly monitored and evaluated on a case-by-case basis and at least every six months.
- All employees 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or codes issued to employees as well as authorizations granted with regard to the processing of personal data will be withdrawn after they leave the company or change responsibilities. Data protection training: Employees are trained annually on data protection and security. In addition to the general training, the special context of the sensitive data of the Aam Digital Case Management System and associated risks and protective measures for this special context are discussed.
- Security Audits: The Aam Digital case management software including its servers and other systems are subject to an extensive annual security audit. This includes the modelling of attack scenarios, the probing of possible security holes (penetration testing), the automatic scanning of systems using tools for security analysis as well as the discussion and adaption of security measures based on these insights. The audit is taking into consideration the guidelines of the German Federal Cyber Security Authority (BSI "IT Grundschutz") and the "Open Web Application Security Project" (OWASP).
- Advice on data reduction: Clients are advised by Aam Digital as a data processor in order to pursue the principles of data economy and only collect such sensitive data that is actually essential for the specific use case.

Entry Control

- Data from the Aam Digital case management system is only stored in ISO 27001 certified data centers in Germany.
- Data centers with strict access control: electronic physical entry control system with log; high security perimeter fencing around the entire data center park; documented distribution of keys to employees and colocation customers; for colocation racks (each Client only for his rack); policies for accompanying and designating guests in the building; data center staff present 24/7; video monitoring at entrances and exits; security door interlocking; systems and server rooms; For people outside of the employment of the data center provider, entrance to the building is only permitted in the company an employee.

Access Control

- Server access strictly restricted: Only a few, carefully selected employees from Aam Digital have access to servers with user data of the Aam Digital case management system as IT administrators. They are trained and committed to the highest confidentiality and security requirements in writing.
- Server access only via SSH with public key: Administrators can only connect to the servers encrypted using the cryptographic network protocol SSH and a private key file with a secure passphrase. 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 weekly basis.
- Software development with highest quality standards: In order to prevent security gaps in the Aam Digital development process, tools for automated code analysis, automated software tests and extensive code reviews by at least one other experienced developer are used.
- Software development with dependency management & updates: Software libraries upon which the Aam Digital case management system is technically based are regularly updated and automatically checked for critical security updates.
- App with password guidelines: A technically integrated password guideline ensures that users can only use passwords that meet minimum requirements in terms of length and complexity. Users can only access the Aam Digital case management system with their individual account and its secure password. Hashed passwords: The Aam Digital case management system only saves passwords as a hash that is calculated using a cryptographic salt value. Should an attacker gain access to a hashed password, the actual password can only theoretically be reconstructed with an immense amount of time and money. In contrast to storing passwords in plain text, this offers the highest possible level of security according to the current state of the art.
- Role-based Access Control: Users can be assigned custom roles to limit access to certain subsets of data for which that user specifically has permission.
- 2-Factor-Authentication: Users can be required to log in with two factors (e.g. an email code) on new devices to prevent use of stolen passwords and increase security.

Usage & Transfer Control

- Transport encryption: Data from the Aam Digital case management system 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 of backups: Backups of data of the Aam Digital case management system 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 employees of Aam Digital 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

- Selection of sub-processors is done under extensive diligence.
- Controlled data processing through other providers: In case third parties are required for processing the data (e.g. data center operators) these are always bound by a data processing agreement in order to ensure all necessary data protection standards and regulations are followed. Clients are informed about the change of such service providers.
- Deleting of data: Client data is deleted 2 years after termination of services or upon request. Processes for processing of beneficiary data: Aam Digital as data processor stores data about beneficiaries of the client. The client is responsible for the legitimacy of the processing of this data. The responsibilities of all parties are agreed upon in a data processing agreement in a clear and transparent way. Support for fulfilling data subjects' requests: As data processor we are supporting our clients in fulfilling their duties to handle requests by affected beneficiaries', whose data is processed by the client using the Aam Digital case management software, in accordance with GDPR regulations. While the client is responsible towards these people according to GDPR, Aam Digital provides any technical support necessary to fulfill these duties.
- Handling data only based on instruction: As data processor our employees at Aam Digital only handle data that the client manages in the Aam Digital case management system on explicit request of the client. These instructions have to be kept in writing. All employees of Aam Digital are participating in related training and bound to this by a written data protection undertaking.
- Instructions are taken in writing.

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: The data in the Aam Digital case management system is automatically backed up to an encrypted file on a daily basis. Data can be restored in the event of technical or user-caused data loss. Backup and recovery concept: The concept for backing up and restoring data is checked regularly. A recovery process is carried out monthly on a trial basis for testing and practice.
- App available offline: The Aam Digital case management system supports extensive offline functionality. Even without a connection to the server - for example if there is temporarily no internet connection available for a user - the data is available locally and the app can still be used.
- 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.