

Data Processing Agreement (DPA)

Version date: October 26th, 2026

Agreement on the processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR)

Between

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

– hereinafter “Provider” –

and

the entity concluding Provider’s Terms of Service (ToS) with Provider

– hereinafter “Customer” –

Preamble

Customer means the natural or legal person that has entered into the Agreement with Provider. Customer shall provide and maintain accurate information reasonably required to identify Customer and, where applicable, the relevant controller, together with relevant contact details for data protection matters.

Customer and Provider have entered an agreement (hereinafter “The Agreement”) regarding the use of the Aam Digital software and, where applicable, related services. Where Provider processes personal data on behalf of Customer in connection with the hosted Service and, where applicable, agreed self-hosted services, this DPA specifies the obligations of the parties regarding such processing in accordance with Article 28 GDPR.

§ 1 Scope, duration and specification of contract processing of Data

1. The processing is based on The Agreement. Agreements on remuneration shall be agreed outside this DPA.
2. This DPA is incorporated into and supplements Provider’s Terms of Service (ToS) and takes effect when The Agreement takes effect. It applies when, and to the extent that, Provider processes personal data on behalf of Customer as a processor under applicable data protection law.
3. Before Provider begins Contract Processing, Customer shall complete the applicable registration or contracting process and provide information reasonably sufficient to identify Customer and, where applicable, the relevant controller. Such information may be provided through Provider’s registration process, an Order Form, or another agreed contracting process. Customer shall keep this information accurate and up to date. This DPA takes effect as stated in § 1.2 and applies to any Contract Processing under The Agreement.
4. This DPA remains in effect during the entire duration of the Agreement. Furthermore, it remains in effect after the Agreement has terminated or expired until the applicable return

and deletion obligations concerning the relevant Data have been completed in accordance with this DPA, including Section 3.10, and applicable law.

5. Customer's data (hereinafter "Data") refers to personal data of data subjects according to the definitions of the GDPR that Customer processes alone or jointly within the scope of the software or requests to be processed on its behalf. The annex "Processing Activities and Type of Data" specifies the subject matter, purpose, categories of data and data subjects of the processing.
6. This DPA shall apply to all activities related to The Agreement, in whose scope Provider processes Data on behalf of Customer as a processor within the meaning of Article 28 GDPR (hereinafter, "Contract Processing").
7. Customer ordinarily acts as "controller" of the Data within the meaning of Art. 4(7) GDPR and remains responsible, in that role, for assessing the permissibility of the processing of Data, including the applicable legal basis under Art. 6 GDPR, and for safeguarding the rights of data subjects, except to the extent Provider has express obligations as processor under this DPA or applicable data protection law. Where Customer processes Data as a processor on behalf of another controller, Customer acts as processor for that processing, represents that it is authorized by the relevant controller to engage Provider as a subprocessor and to issue the instructions contemplated by this DPA, and shall ensure that its instructions to Provider are consistent with the underlying controller's instructions. References in this DPA to Customer's controller responsibilities apply in that case only to the extent relevant to Customer's role as processor or responsibilities delegated to it by the underlying controller. Provider may provide documentation or information relevant to Provider's processor role as described in this DPA.
8. Provider acts as "processor" within the meaning of Art. 4(8) GDPR where Customer acts as controller and as a further processor or subprocessor where Customer acts as processor on behalf of another controller. Provider processes the Data on behalf of Customer and, where applicable, the underlying controller in accordance with this DPA.
9. Unless expressly agreed or disclosed otherwise in the applicable Order Form, this DPA, the Standard Subprocessor List, a Customer-Specific Subprocessor authorization, or another binding document, Provider's standard service model is to host Customer Content and operate the production environment for the Service exclusively within the EU/EEA. Provider-controlled processing under this 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. For clarity, Provider-controlled processing may include remote access to Customer Content or personal data by Provider personnel or other persons acting under Provider's authority where such access is necessary to provide, secure, maintain, or support the Service. The foregoing location commitment applies to processing locations controlled or selected by Provider. It does not restrict the locations from which Customer or Authorized Users access the Service, the locations of Customer- or Authorized User-controlled devices on which Data may be stored through offline-first functionality, or Customer-directed retrieval, export, API use, email notification, integration, or other transmission of Data to systems, recipients, or destinations selected or controlled by Customer or its Authorized Users. Provider-controlled processing outside the EU/EEA remains subject to technical feasibility, applicable data protection law, Customer's documented instructions where required, the

agreed subprocessor authorization mechanism, and any required GDPR transfer safeguards.

10. Customer-directed functionality and access. Where Customer or an Authorized User with the required permissions configures or uses API, reporting, export, notification, integration, or similar functionality, or where Customer authorizes an Authorized User to access or synchronize Data from a location outside the EU/EEA, such configuration, authorized use, access, or synchronization constitutes Customer's documented instruction to Provider to make the selected Data available or transmit or synchronize it as necessary. Customer is responsible for determining which Data is made available, selecting and authorizing recipients and destinations, protecting API credentials, authorizing access by its Authorized Users, and complying with applicable law in relation to Customer-directed onward disclosure, storage, access, synchronization, or processing. Customer is responsible for determining whether Customer-authorized access or synchronization from outside the EU/EEA, or subsequent processing, constitutes a transfer under Chapter V GDPR and, where applicable, for ensuring compliance with applicable Chapter V requirements. Provider does not select, approve, monitor, or control Customer-selected systems, recipients, destinations, or Customer- or Authorized User-controlled access locations and is not required to independently determine their location, identity, or legal status except to the extent required by applicable law. Nothing in this paragraph excludes obligations imposed directly on Provider by applicable law. Where Provider believes that a Customer instruction would infringe applicable law, § 3.1 applies.

§ 2 Representation and information accuracy

1. Customer enters into this DPA on its own behalf or, where applicable, on behalf of the legal entity it represents.
2. Customer represents that the information provided during account registration or another applicable contracting process is accurate and sufficient to identify Customer and, where applicable, the relevant controller.
3. Customer shall ensure that the contact information associated with the account remains accurate and up to date.
4. Customer shall provide additional identifying information upon reasonable request where necessary for compliance with applicable data protection law.

§ 3 Provider's obligations

1. Provider shall process personal data only within the scope of The Agreement and Customer's documented instructions, except where Union or Member State law requires Provider to process Data otherwise. Where such a legal requirement applies, Provider shall inform Customer of that legal requirement before the relevant processing, unless the law prohibits such information on important grounds of public interest. Where Provider believes that an instruction would infringe applicable law, Provider shall notify Customer of that belief without undue delay and may suspend performance of the relevant instruction until Customer modifies or withdraws it, or Provider otherwise determines that the instruction may lawfully be performed.
2. No ownership transfer; no sale or independent use. As between Customer and Provider, Customer retains all rights and control over Customer Content (as defined in The Agreement) and Data. Provider does not acquire ownership rights in Customer Content or Data. Provider shall not sell, rent, commercially exploit, or use Data for advertising, profiling, or model training. Provider may disclose Data only as expressly instructed by

Customer, as permitted by The Agreement for the provision, security, maintenance, and support of the Service, or as required by applicable law, subject to § 3.1.

3. Provider shall, within Provider's scope of responsibility, organise Provider's internal organisation so it satisfies the specific requirements of data protection. Provider shall implement technical and organizational measures to ensure the adequate protection of Customer's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Provider shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. These measures are specified in the annex "Technical and Organizational Measures," which forms part of this DPA. Customer acknowledges that the applicable technical and organizational measures are agreed as part of this DPA and that Customer, in its role as controller, remains responsible for determining whether those measures are appropriate for Customer's processing activities and risk profile. Provider reserves the right to modify the measures and safeguards implemented, provided that the level of security shall not be materially less protective than initially agreed.
4. Taking into account the nature of the processing and the information available to Provider, Provider shall assist Customer in fulfilling data subjects' requests and in meeting Customer's obligations under Articles 32 to 36 GDPR, as required by Article 28(3) GDPR. Provider may make standard guidance, documentation, or compliance information available to support Customers in understanding these responsibilities. Unless caused by Provider's breach of this DPA or applicable law, extraordinary assistance beyond Provider's standard support and compliance processes may be subject to reasonable additional charges agreed with Customer.
5. Provider warrants that all employees involved in Contract Processing of Customer's Data and other such persons as may be involved in Contract Processing within Provider's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Provider warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.
6. Provider shall notify Customer without undue delay after becoming aware of a personal data breach affecting Data within Provider's scope of responsibility. To the extent known and reasonably available, Provider shall provide information reasonably required to assist Customer with its obligations under Articles 33 and 34 GDPR, including the nature of the breach, the categories and approximate number of affected data subjects and personal data records where available, the likely consequences, and the measures taken or proposed to address and mitigate the breach. Provider may provide information in phases as it becomes available. Provider shall implement the measures necessary for securing Data and mitigating potential negative consequences for data subjects and shall coordinate such efforts with Customer without undue delay.
7. Provider shall make available to Customer a contact point for data protection matters arising out of or in connection with The Agreement. Provider may make this contact point available through its website, the Service, the DPA, or other customer-facing documentation.
8. Provider warrants that Provider fulfills its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

9. Provider shall correct or erase Data if so instructed by Customer and where such instruction is consistent with The Agreement and applicable law. Where erasure or restriction of processing is not possible in a particular case, including because data remains in backups until overwritten or deleted under the applicable backup lifecycle or because retention is required by law, Provider shall inform Customer and handle the data in accordance with applicable law and The Agreement. Any separate remuneration for non-standard return, extraction, storage, handover, restore, or other customer-requested operational assistance shall be governed by The Agreement or otherwise agreed separately, except that Provider shall not impose switching charges for actions it is required to perform without charge under applicable EU Data Act switching rules. Where Data has previously been stored locally on Customer- or Authorized User-controlled devices through the Service's offline-first functionality, Provider cannot independently access or remotely erase that local copy. In normal use, server-side deletions and other relevant changes are ordinarily reflected in locally stored Data when the relevant Authorized User is logged into the Service on that device and the application successfully synchronizes. However, server-side deletion, a deletion instruction, 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 is responsible for appropriate device management and local deletion where required.
10. Upon termination of Contract Processing, whether in whole or in relation to one or more Customer Instances or another identifiable processing scope, Provider shall, at Customer's choice, delete or return the Data relating to the terminated processing scope in accordance with Customer's instructions, the applicable data export, retention and deletion provisions of the Agreement, and applicable law. Customer may communicate its choice before termination or during the applicable ordinary post-termination retention period. Where Customer timely requests return before the end of the applicable post-termination retention period, Provider will retain the Data reasonably necessary to fulfil that request until the standard return package has been made available to Customer and Customer has had a reasonable opportunity to retrieve it. Where Customer requests return, Provider will make the relevant Data available through Provider's then-current standard return method. The standard return package consists of the standard database export made available through the Service, together with Customer-uploaded files or attachments that form part of the relevant Data, where applicable. Provider is not required as part of this standard return to provide custom formats, selective extraction, data transformation, destination-side migration, or other non-standard assistance. Provider will not charge an additional fee for providing the standard return package to the extent such return is required under this DPA or applicable law. Additional return, retrieval, extraction, transformation, storage, handover, migration, or other non-standard operational assistance may be subject to additional fees, provided that the applicable fee or, where the total fee cannot reasonably be determined in advance, the basis for calculating the fee is communicated in advance and agreed with Customer before the chargeable assistance is provided. If Customer has not requested return by the end of the applicable post-termination retention period and has not instructed earlier deletion, Customer instructs Provider to delete the relevant Data in accordance with the Agreement and applicable law. After return, Provider will delete remaining Provider-controlled copies in accordance with the applicable deletion and backup lifecycle, unless retention is required by Union or Member State law. Upon Customer's reasonable request, Provider will confirm completion of the applicable deletion from Provider-controlled active

systems. Data remaining in backups will continue to be protected and deleted or overwritten in accordance with the applicable backup lifecycle, unless longer retention is required by Union or Member State law. Mandatory switching, portability, retrieval and erasure obligations under applicable law remain unaffected. This DPA remains applicable to the relevant Data until the applicable return and deletion obligations have been completed in accordance with this Section and applicable law. Server-side deletion does not by itself erase Data previously stored on Customer- or Authorized User-controlled devices through the Service's offline-first functionality; such copies remain subject to the applicable provisions of the Agreement concerning local-device copies.

11. Where a data subject asserts claims against Customer in accordance with Article 82 GDPR, Provider shall provide reasonable assistance to Customer, taking into account the nature of the processing, the information available to Provider, and Provider's scope of responsibility, to the extent required by applicable data protection law. Assistance beyond Provider's standard compliance processes may be subject to reasonable additional charges unless the claim was caused by Provider's breach of this DPA or applicable law. The applicable charge or, where the total charge cannot reasonably be determined in advance, the applicable basis for calculating the charge, such as an hourly or daily rate, shall be communicated in advance and agreed with Customer before the chargeable assistance is provided.

§ 4 Customer's obligations

1. Where Customer acts as controller, Customer is solely responsible for the legal basis of processing the Data and for safeguarding the rights of data subjects in the relationship between the parties. Where Customer acts as processor on behalf of another controller, Customer is responsible for ensuring that it acts within the underlying controller's instructions and authority and that Provider's processing is covered by the applicable instructions and authorization; responsibilities allocated by applicable law to the underlying controller remain with that controller.
2. Customer shall notify Provider, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Customer in the results of Provider's work.
3. Where a data subject asserts claims against Provider in accordance with Article 82 GDPR that relate to Customer's Data, Customer shall provide reasonable assistance to Provider, taking into account Customer's role in the relevant processing chain, the nature of the processing, and the information available to Customer, to the extent required by applicable data protection law.
4. Customer shall notify Provider of the point of contact for any issues related to data protection arising out of or in connection with The Agreement.
5. If Provider is obliged to provide information about the processing of Customer's Data to a government agency or person, or to cooperate with these agencies in any other way, Customer is obliged to support Provider in providing such information or fulfilling other obligations to cooperate.

§ 5 Enquiries by data subjects

1. Where a data subject asserts claims for rectification, erasure or access against Provider, and where Provider is able to correlate the data subject to Customer, based on the information provided by the data subject, Provider shall refer such data subject to Customer. Provider shall forward the data subject's claim to Customer without undue delay.

2. Taking into account the nature of the processing and the information available to Provider, Provider shall assist Customer with data-subject enquiries addressed to Provider as required by Article 28(3) GDPR. Provider shall not be liable to the extent Customer's failure to respond to a data subject's request in full, correctly, or in a timely manner is attributable to Customer, without limiting Provider's responsibility for its own breach of this DPA or applicable law.

§ 6 Documentation

1. Provider shall document and upon Customer's request prove compliance with the obligations agreed upon in this DPA by appropriate measures.
2. Audits and inspections by Customer or an auditor appointed by Customer shall, where reasonably necessary, be conducted during regular business hours, without unreasonably interfering with Provider's operations, upon prior notice, and subject to appropriate confidentiality safeguards protecting other customers and Provider's confidential information. Provider may object to auditors who are competitors of Provider. Provider may satisfy audit requests through current certifications, audit reports, or other standard compliance documentation where these reasonably address Customer's request. Provider may charge reasonable fees for audit support that exceeds such standard documentation or materially exceeds ordinary effort, except where the audit is required due to a material personal data breach, credible evidence of material non-compliance, or a request by a competent supervisory authority. Any applicable fee or, where the total fee cannot reasonably be determined in advance, the basis for calculating the fee will be communicated to Customer in advance before chargeable additional audit support is provided.
3. Where a data protection supervisory authority or another supervisory authority with statutory competence for Customer conducts an inspection, the procedural safeguards in §6.2 shall apply mutatis mutandis to the extent legally permissible. A confidentiality undertaking shall not be required where the authority is subject to professional or statutory confidentiality obligations.

§ 7 Subprocessors

1. Customer generally authorizes Provider to engage the subprocessors identified in Provider's List of Standard Subprocessors at <https://www.aam-digital.com/legal/subprocessors> (the "Standard Subprocessor List") as further processors for the processing of personal data under this DPA (the "Standard Subprocessors"). The Standard Subprocessor List forms part of this DPA and identifies the Standard Subprocessors used by Provider at the relevant time.
2. Provider may additionally engage a subprocessor solely in relation to processing for a particular Customer (a "Customer-Specific Subprocessor") where Customer has specifically authorized that subprocessor in writing or text form, including electronic form, before the relevant processing begins. Such specific authorization may be given in a Customer-Specific Subprocessor Annex to this DPA, an Order Form, or another binding document that identifies the subprocessor and describes the processing entrusted to it. Customer-Specific Subprocessors need not be included in the public Standard Subprocessor List unless they are also used as Standard Subprocessors.
3. Provider will ordinarily give Customer at least fifteen (15) working days' prior notice before engaging a new or replacement Standard Subprocessor. Notice will be sent to Customer's designated data-protection contact or, if none is available, to an account/admin contact or

another agreed electronic notice channel. Customer may object to a new or replacement Standard Subprocessor during the applicable notice period if Customer has a materially important data protection reason for the objection. Provider may use a shorter notice period where reasonably necessary for security, continuity, or urgent operational reasons. In such cases, Provider will give Customer as much prior notice as reasonably practicable and will identify the shorter applicable objection period in the notice. The new or replacement Standard Subprocessor will not begin processing Data until the applicable objection period has expired without objection or Customer has otherwise authorized the engagement. If Customer does not object within the applicable period, Provider may engage the new or replacement Standard Subprocessor. If Customer raises a justified objection and the parties cannot resolve the issue amicably, Customer may terminate the affected services or, if reasonably necessary, The Agreement. Any addition or replacement of a Customer-Specific Subprocessor requires Customer's prior specific authorization in writing or text form, including electronic form, before that subprocessor begins the relevant processing. For all subprocessors, Provider shall enter into the contractual arrangements required by Article 28(4) GDPR, ensure that the applicable data protection obligations resulting from The Agreement and this DPA are valid and binding upon the subprocessor, and remain responsible for the performance of its subprocessors in accordance with applicable law. Provider shall keep information identifying the subprocessors engaged for Customer and the processing entrusted to them up to date and available to Customer.

§ 8 Obligations to inform, form requirements, choice of law

1. Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Provider's control, Provider shall notify Customer of such action without undue delay. To the extent legally permitted, Provider shall notify the relevant third parties that the affected Data is processed by Provider on behalf of Customer and, where applicable, the underlying controller, and that Customer acts as controller or processor in the relevant processing chain as applicable.
2. No modification of this DPA or any of its components, including Provider's representations and warranties, if any, shall be valid and binding unless made in writing or text form, including electronic form, and expressly states that it applies to this DPA. The same form requirement applies to any waiver or modification of this form requirement.
3. In case of any conflict, the data protection regulations of this DPA shall take precedence over the regulations of The Agreement. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.
4. All annexes of this DPA shall form part of this DPA.
5. This DPA is subject to the laws of Germany.

This DPA is entered into with effect from the date on which The Agreement takes effect.

Annexes to this DPA

- Processing Activities and Type of Data

- List of Standard Subprocessors (available at <https://www.aam-digital.com/legal/subprocessors>) and any Customer-Specific Subprocessor Annexes or other specific written authorizations agreed with Customer
- List of Technical and Organizational Measures (TOMs)

Annex Processing Activities and Type of Data:

Subject matter

The provision and operation of one or several Aam Digital software systems and related services agreed with Customer, including, where applicable, support, implementation, configuration, data migration, and technical assistance. The software is highly customizable and allows Customer and its users to record, manage, and analyse data for Customer's chosen purposes.

Nature of processing

Hosting, storing, organizing, structuring, retrieving, accessing, viewing, configuring, importing, exporting, transmitting, transforming, testing, troubleshooting, backing up, restoring, deleting, or otherwise handling Data as necessary to provide and operate the Service and perform related agreed services.

Purpose of the processing

Provider processes Data for purposes determined by Customer through Customer's configuration and use of the Aam Digital software system(s) and the services requested from Provider. Customer as controller or, where Customer acts as processor, the relevant underlying controller determines the purposes of the processing. Provider processes Data to provide, operate, secure, maintain, and support the Service and to perform related agreed services, including, where applicable, support, implementation, configuration, data migration, and technical assistance, in accordance with Customer's documented instructions, The Agreement, and applicable law.

Categories of data

The Service is highly configurable. Provider does not determine which categories of personal data Customer chooses to process through the Service. Depending on Customer's configuration, data model, use of the Service and documented instructions, Data may include any category of personal data that Customer chooses to enter, upload, import, generate, store or otherwise process through the Service. Such Data may include, for example, identification and contact data; demographic and household information; case-management, service-delivery, project and program records; activity, attendance and participation information; notes, assessments, documents, files and communications; financial or socioeconomic information; and other Customer-defined fields, records and information.

Where Customer chooses to process such Data, Data may also include special categories of personal data under Article 9 GDPR, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data, biometric data processed for the purpose of uniquely identifying a person, health data, and data concerning a person's sex life or sexual orientation. Data may separately include personal data relating to criminal convictions and offences under Article 10 GDPR. Because many Customers work with sensitive communities, Provider's processor role is supported by the technical and organizational measures described in the Technical and Organizational Measures (TOMs), which form part of this DPA. Customer remains responsible for determining the lawful and appropriate use of the system for the relevant data subjects and use case, subject to the role allocation described in this DPA.

Separately, where processed on behalf of Customer, the processing may also include personal data generated or processed in connection with the provision, security, maintenance, support, and operation of the Service, such as Authorized User account data, authentication data, role/permission data, audit/log data, support-related data, usage data, technical data, notification data, and error-monitoring data. To the extent Provider processes similar data for its own controller-side purposes, such processing is governed by Provider's applicable privacy policy rather than this DPA.

Data subjects

The categories of data subjects are determined by Customer's configuration and use of the Service and, where Customer acts as processor, by the underlying controller's instructions. They may include, for example, beneficiaries, participants, clients, members, applicants, household or family members, children or other minors, students, mentors, mentees, employees, contractors, volunteers, partners, donors, contacts, Authorized Users, and any other individuals whose personal data Customer chooses to process through the Service.