AITY DOCUMENTS

AITY CLOUD SRL

Data Processing Agreement (DPA)

Version 1.0 · effective from 15 August 2026 · aity.tech/documents

DENUMIRE / ENTITY	AITY CLOUD SRL
CUI	39458128 (RO39458128)
NR. REG. COM.	J2018000824245
EUID	ROONRC.J2018000824245
CORESPONDENȚĂ / CORRESPONDENCE	Str. Heliade Între Vii nr. 35, cod 023382, Sector 2, București, România
CONTACT	office@aity.ro · support@aity.ro · aity.ro · aity.tech

(c) AITY CLOUD SRL

Table of contents

Data Processing Agreement (DPA)

VERSION 1.0 · EFFECTIVE FROM 15 AUGUST 2026 · AITY CLOUD SRL

Romanian version · Download PDF

This Data Processing Agreement (the "**DPA**") forms part of the contract between **AITY CLOUD SRL**, a Romanian limited liability company, with its registered office at SACEL no. 1003, Săcel Village, Săcel Commune, Maramureș County, postal code 437290, Romania, tax ID 39458128 (VAT RO39458128), Trade Register J2018000824245, EUID ROONRC.J2018000824245, subscribed and paid-up share capital RON 5,000, correspondence address Str. Heliade Între Vii no. 35, postal code 023382, Sector 2, Bucharest, Romania, telephone +40735850896 (Monday-Friday, 09:00-18:00 Romanian time), e-mail office@aity.ro ("**aity**", the "**Processor**") and the Customer, concluded under the Terms of Service (the "**Terms**"), and governs, pursuant to article 28 of Regulation (EU) 2016/679 ("**GDPR**"), aity's processing, on the Customer's behalf, of personal data contained in Customer Content ("**Customer Data**"). The Romanian and English versions are both official; in case of divergence, the Romanian version prevails.

1. Scope and roles

1.1. This DPA applies automatically, without a separate signature, only to the extent that the Customer acts as a controller or processor subject to the GDPR and aity processes Customer Data on its behalf. If the Customer is another controller's processor, it warrants that the instructions given to aity are authorized by that controller. Roles are determined by the actual processing, not only by contractual designation. The processing of content used by Consumers exclusively for personal or household purposes is described in the Privacy Policy.

1.2. The DPA does not apply to data for which aity is a controller (account data, billing, platform logs), described in the Privacy Policy.

1.3. In the event of conflict, the DPA prevails over the other Contract Documents only with respect to the protection and processing of Customer Data. The DPA does not extend aity's liability or modify commercial terms unless it expressly provides for a derogation applicable to the relevant subject matter.

2. Details of processing

The details of processing are set out in Annex 1. The duration of processing is the term of the contract, plus the Retrieval Period and the deletion and backup rotation periods under article 11.

3. Customer instructions

3.1. aity processes Customer Data only on the Customer's documented instructions, including with respect to transfers, for the purpose of providing, securing, and monitoring the Services. The documented instructions are: (a) the Contract Documents; (b) the Customer's and its End Users' use and configuration of the Services, including recipients, export destinations, and deletion commands; (c) other written instructions agreed by the parties. aity may process Customer Data outside these instructions only if required to do so by Union or Member State law applicable to it; in that case, it informs the Customer of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

3.2. aity informs the Customer **immediately** if, in its opinion, an instruction infringes the GDPR or other data protection provisions and may suspend performance of the instruction until clarification, without being required to conduct an exhaustive legal analysis.

3.3. aity does not use Customer Data for advertising, commercial profiling, market research, or other purposes of its own and does not sell that data.

4. Confidentiality

Persons authorized by aity to process Customer Data are subject to contractual or statutory confidentiality obligations, and their access is limited to what is necessary to provide, secure, and monitor the Services.

5. Security

5.1. aity implements and maintains the technical and organizational measures described in Annex 2, ensuring a level of security appropriate to the risk under article 32 GDPR.

5.2. The Customer is responsible for secure use of the Services on its side: managing credentials and access roles, appropriately configuring the Services, securing its own systems and applications for aity Cloud, and making its own backups under the Terms. Before processing, the Customer informs aity of special risks or legal requirements that do not reasonably arise from ordinary use. aity may update the measures in Annex 2 to reflect technical developments without materially reducing the overall level of security during the Services.

6. Sub-processors

6.1. The Customer generally authorizes the use of sub-processors for processing Customer Data. The current list, service categories, locations, and date from which each sub-processor is authorized are set out in Annex 3. The statement "none" is a valid situation on the version date, not a commitment that aity will not use EEA infrastructure or backup partners in the future.

6.2. aity directly notifies the Customer by e-mail at least **15 (fifteen) days** before authorizing a new sub-processor for Customer Data, stating its identity, country, service, and intended processing. The Customer may submit a reasoned objection within that period; the parties first attempt a reasonable solution. If the objection cannot be resolved, the Customer may terminate the affected Service without penalty until the activation date, which is the Customer's exclusive contractual remedy for the objection.

6.3. Every sub-processor is bound by written contract to the applicable obligations under article 28(4) GDPR, and aity remains fully liable to the Customer for their performance. Upon request, aity supplies a redacted copy of the relevant data protection clauses and may remove confidential information, trade secrets, and other customers' data.

7. Assistance

7.1. Taking into account the nature of processing, aity assists the Customer, through appropriate technical and organizational measures (including the Services' search, export, and deletion features), in fulfilling its obligation to respond to data subject requests. If a data subject contacts aity directly regarding Customer Data, aity will direct that person to the Customer and will not respond on the merits without the Customer's instructions, except where required by law.

7.2. aity reasonably assists the Customer in complying with articles 32-36 GDPR (security, breach notification, impact assessment, consultation with the authority), taking into account the information available to it. For assistance exceeding the standard features of the Services and a reasonable effort, aity may charge a fee communicated in advance.

8. Personal data breaches

aity notifies the Customer without undue delay after becoming aware of any personal data breach affecting Customer Data, providing the information required by article 33(3) GDPR as it becomes available and reasonably cooperating in investigation and remediation. aity's notification or response to an incident does not constitute an admission of fault or liability. aity has no obligation to examine the content of Customer Data to identify information subject to specific legal requirements; the Customer remains responsible for its notification obligations to authorities and data subjects.

9. Data location and transfers

9.1. Customer Data stored at rest through the Services is kept in the European Economic Area, on infrastructure operated by aity or the sub-processors in Annex 3. Administrative access follows the same location limits, except for a transfer documented and protected under this article.

9.2. Transmission by aity, on the Customer's behalf, of a message, export, or other set of Customer Data to a recipient, provider, or destination in a third country may constitute a transfer within the meaning of Chapter V GDPR. aity acts only on the Customer's documented instructions and applies the mechanism under its control that is appropriate to the destination and flow. The Customer ensures that the instruction, recipients, and subsequent use comply with its obligations. If no lawful mechanism is available for a regular transfer, aity may refuse or suspend the instruction. Messages received from a third country by aity infrastructure in the EEA are assessed separately from the outbound flow.

9.3. Any other processing outside the EEA takes place only on the basis of an adequacy decision or an appropriate safeguard under article 46 GDPR, following assessment of the transfer and application of necessary supplementary measures, and after following article 6.2 for a new sub-processor. Upon request, aity makes a copy or description of the safeguard available to the Customer, subject to necessary redactions.

10. Audit

10.1. aity makes available to the Customer the information necessary to demonstrate compliance with article 28 GDPR: this DPA, the description of the measures in Annex 2, and available reports, certifications, or attestations.

10.2. To the extent that the information in article 10.1 is not reasonably sufficient, the Customer may conduct an audit, including an inspection, directly or through a mandated independent auditor that is not an aity competitor. The audit takes place no more than once in any 12-month period, on 30 days' prior notice and during business hours. The frequency limit and notice do not apply to the extent the audit is required by a competent authority, follows a significant incident, is urgent to protect data subjects, or the Customer presents reasonable evidence of material non-compliance. The audit does not permit access to other customers' data or information that would compromise security; confidentiality obligations apply, and the scope, timing, and duration are reasonably coordinated. Costs are borne by the Customer, including the reasonable cost of aity's time beyond one business day, except to the extent the audit proves material non-compliance attributable to aity.

11. Deletion and return of data

Upon termination of the Services, the Retrieval Period in the Terms applies. Before it expires, the Customer may choose to have the data returned by export and/or deleted early. After expiry, aity deletes Customer Data from primary systems within no more than 30 days, except where retention is required by Union or Member State law. Deletion includes all existing copies; backups are isolated from current use and removed no later than expiry of the 45-day rotation cycle after deletion of primary data. Data retained by law is protected, logically separated, and used only for that purpose. Upon request, aity confirms completion of deletion in writing.

12. Liability

Each party's total liability under this DPA is subject to the limitations and exclusions of liability in the Terms, to the extent permitted by law; nothing in this DPA limits data subjects' rights or the parties' liability towards them under article 82 GDPR.

13. Duration

The DPA remains effective for as long as aity processes Customer Data and expires automatically upon completion of the deletion under article 11.

Annex 1 - Details of processing

ELEMENT	DESCRIPTION
Subject matter	Provision of the aity Platform (e-mail and collaboration) and aity Cloud (cloud infrastructure) services
Nature of processing	Technical collection, hosting, organization, storage, transmission, backup, recovery, display, export, and deletion, in accordance with the Customer's use and instructions
Purpose	Providing, securing, and monitoring the Services under the contract
Categories of data subjects	The Customer's End Users; their correspondents; persons whose data the Customer includes in hosted content
Categories of data	Data included by the Customer in Customer Content: identification and contact data, communications content, files, and any other data the Customer chooses to store or transmit. The Customer is responsible for not storing data for which the law imposes requirements the Services do not meet.
Special categories	Only if and to the extent that the Customer includes them in its content, under its responsibility

Annex 2 - Technical and organizational measures

- keeping Customer Data stored at rest in the EEA and applying appropriate contractual and physical measures for infrastructure locations;
- redundant architecture for components declared to be highly available, restricted-access backups, documented rotation cycles, and periodic restoration tests;
- TLS for external connections and internal flows where appropriate, protection of secrets and keys, and access controls for storage media;
- role-based, least-privilege, and need-to-know access control; strong authentication for administrative access and periodic review of rights;
- network segmentation, access policies, firewall, and anti-malware, anti-phishing, and anti-spam protections appropriate to the Service;
- continuous infrastructure monitoring, logging with data minimization and without copying confidential query parameters into telemetry, vulnerability management, and security updates;
- incident response, continuity, recovery, and breach notification procedures;
- deletion of primary data and expiry of backups under article 11, with records and confirmation upon request;
- periodic testing, assessment, and evaluation of the effectiveness of measures, including internal reviews, scans, and security testing;
- pseudonymization and minimization where appropriate to the nature of processing; staff training and confidentiality obligations.

Annex 3 - Sub-processors

Register valid on 16 August 2026: no external sub-processor is active for ordinary storage of Customer Data. Data is operated in the EEA by aity. Any EEA infrastructure or backup partner will be added here, with name, country, service, and authorization date, only after the notice under article 6.2.

PayU, SmartBill, identity providers, and other recipients of data for which aity is a controller do not become sub-processors merely through their use; their roles and flows are described separately in the Privacy Policy.

Version history

VERSION	DATE	CHANGES
1.0	15 August 2026	First published version.