

Data Processing Agreement

Effective date: 1 November 2026 · Version 1.0

This Data Processing Agreement ("DPA") forms part of the contract between the customer ("Controller") and DATATIP CZ, s.r.o., Pelušková 1443, 198 00 Praha 14, Czech Republic, ID No. 24853577 ("Processor") and sets out the terms required by Article 28(3) of Regulation (EU) 2016/679 ("GDPR").

1. Subject matter

The Processor processes personal data on behalf of the Controller to the extent necessary to provide the Baaito service under the contract.

2. Duration

This DPA applies for the term of the contract and for as long as the Processor processes personal data on behalf of the Controller, including the export and deletion period under Section 12.

3. Nature and purpose of processing

Processing consists of storing, organising, retrieving, transmitting to enabled services and deleting personal data for the purposes of document preparation, conversations with the Baaito assistant and search in sources provided by the Controller.

4. Categories of data and data subjects

- Data subjects: the Controller's users; persons named in the Controller's documents and sources.
- Categories of data: identification and contact data, organisational and role data, and any personal data contained in conversations, documents, uploaded sources and generation inputs and outputs.
- The Controller shall not submit special categories of personal data unless it has a legal basis and has assessed the risks.

5. Processing on documented instructions

The Processor processes personal data only on documented instructions of the Controller, including with regard to transfers to third countries, unless required by EU or Member State law; in that case it informs the Controller before processing unless the law prohibits it. The contract, this DPA and the settings made by the Controller's administrators in the service (such as enabled AI models and integrations) are the Controller's instructions. The Processor informs the

Controller if it believes that an instruction infringes data protection law.

6. Confidentiality of personnel

The Processor ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7. Technical and organisational measures

The Processor implements the measures set out in Annex 2 and keeps them appropriate to the risk in accordance with Article 32 GDPR.

8. Sub-processors

The Controller gives a general authorisation to engage the sub-processors listed at /legal/subprocessors (<https://baaito.app/legal/subprocessors>). The Processor informs the Controller of any intended addition or replacement at least 30 days in advance; the Controller may object on reasonable data protection grounds within that period. If no solution is found, the Controller may terminate the affected service. The Processor imposes on each sub-processor data protection obligations equivalent to this DPA and remains liable for its performance.

9. International transfers

Personal data is transferred outside the EU/EEA only on the basis of an adequacy decision or the Standard Contractual Clauses (Module 3, processor to processor) with supplementary measures where needed.

10. Assistance to the Controller

Taking into account the nature of processing, the Processor assists the Controller with appropriate measures in responding to requests from data subjects, and with data protection impact assessments, prior consultations with supervisory authorities and the Controller's other obligations under Articles 32 to 36 GDPR.

11. Personal data breach

The Processor notifies the Controller of a personal data breach without undue delay and at the latest within 48 hours after becoming aware of it, with the information available at the time, and provides further information as it becomes available.

12. Return and deletion

After the contract ends, the Controller may export its data for 30 days. The Processor then deletes the personal data; backup copies are deleted within 35 days, unless EU or Member State law requires storage.

13. Audits

The Processor makes available the information necessary to demonstrate compliance with Article 28 GDPR, primarily through certificates, reports and answers to security questionnaires. Where this is not sufficient, the Controller may carry out an on-site audit with reasonable prior notice, during business hours and at its own cost, subject to confidentiality.

Annex 1 – Description of processing

Item	Description
Subject matter	Provision of the Baaito document workspace
Purpose	Document preparation, conversations with the assistant, search in Controller sources
Data subjects	Controller users; persons named in Controller documents and sources
Data categories	Identification, contact and role data; personal data in workspace content
Duration	Term of the contract plus the export and deletion period
Sub-processors	See /legal/subprocessors

Annex 2 – Technical and organisational measures

- Encryption of data in transit (TLS).
- Logical separation of data per organisation and role-based access control.
- Audit logging of security-relevant and administrative actions.
- Encrypted storage of secrets and connector credentials.
- Backups kept for 35 days.
- Documented incident handling, including breach notification within 48 hours.