Data Processing Agreement

v0.1 draft · jul 2026

Data Processing Agreement — Innovatica

> **DRAFT — NOT FOR USE WITH CLIENTS YET.** Structured on Article 45 of the Serbian Law on Personal Data Protection ("**ZZPL**") and Article 28 GDPR. It **must be reviewed by qualified legal counsel admitted in the Republic of Serbia** before first client use — in particular the international-transfer mechanism in Section 7 and the annexes. Bracketed items are placeholders.

1. Parties, roles and purpose

1.1. This Data Processing Agreement (the "**DPA**") is an annex to the service contract (the "**Contract**") between **Innovatica** [full legal name, matični broj, PIB, seat] (the "**Processor**") and the client identified in the Offer (the "**Controller**").

1.2. For personal data processed in delivering the Services, the Client acts as **controller** and Innovatica as **processor** within the meaning of the ZZPL and, where applicable, the GDPR. This DPA is the written agreement required by Art. 45 ZZPL (Art. 28(3) GDPR).

1.3. Terms not defined here have the meaning given in the ZZPL; "personal data", "processing", "data subject" and "personal data breach" are used as defined there.

2. Subject matter, duration, nature and purpose

2.1. **Subject matter and nature:** hosting and operating the contracted Services — AI assistants and chat agents, web applications, collection and analysis of publicly available web data, reporting — including storage, retrieval, analysis, logging and transmission of the personal data described in Annex 1.

2.2. **Purpose:** delivery of the Services under the Contract; no other purpose. The Processor does not sell personal data and does not use it to train its own or third parties' machine-learning models. Third-party AI providers used at inference time are contractually bound not to train on submitted content (Annex 3).

2.3. **Duration:** the term of the Contract, plus the wind-down period in Section 8.

2.4. **Types of data and categories of data subjects:** as described in Annex 1, completed per engagement.

3. Instructions

3.1. The Processor processes personal data **only on the Controller's documented instructions** — the Contract, this DPA, its annexes and the Service configuration jointly constitute the standing instructions — including with regard to transfers to third countries, unless processing is required by the

law applicable to the Processor; in that case the Processor informs the Controller before processing, unless that law prohibits it.

3.2. The Processor informs the Controller without delay if, in its opinion, an instruction infringes the ZZPL, the GDPR or other data-protection law, and may suspend execution of that instruction until it is confirmed or changed.

4. Confidentiality and personnel

Persons authorised to process personal data are bound by contractual or statutory confidentiality, are limited to what their role requires, and are trained appropriately for their duties.

5. Security of processing

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks for data subjects, the Processor implements appropriate technical and organisational measures under Art. 50 ZZPL (Art. 32 GDPR). The measures in place at signature are described in **Annex 2**; the Processor may update them provided the overall security level is not reduced.

5.2. The Processor assists the Controller, insofar as possible and at the Controller's reasonable cost for material effort, with: responding to data subjects' requests (access, rectification, erasure, restriction, portability, objection); security of processing; breach notification; data-protection impact assessments and prior consultations with the supervisory authority.

6. Personal data breaches

The Processor notifies the Controller **without undue delay after becoming aware of a personal data breach** affecting the Controller's personal data, and in any case within [48] hours of becoming aware, providing the information the Controller needs for its own notification duties (nature of the breach, categories and approximate numbers of data subjects and records, likely consequences, measures taken or proposed), supplemented as it becomes available. Notification to the supervisory authority and to data subjects is the Controller's responsibility unless agreed otherwise.

7. Subprocessors and international transfers

7.1. The Controller grants a **general authorisation** for the engagement of the subprocessors listed in **Annex 3**. The Processor informs the Controller of intended additions or replacements at least [15] days in advance; the Controller may object in writing on reasonable data-protection grounds, in which case the parties seek a solution and, failing one, the Controller may terminate the affected Service.

7.2. The Processor imposes on every subprocessor, by written contract, data-protection obligations no less protective than this DPA, and remains fully liable to the Controller for the subprocessor's performance.

7.3. **Location of processing.** Primary processing and storage run in the European Union (Microsoft Azure, EU regions — currently Sweden Central). Some subprocessors process limited data outside Serbia and the EU (Annex 3 — e.g. AI inference in the United States).

7.4. **Transfer mechanism.** Transfers from Serbia are made under Art. 63–65 ZZPL: to states on Serbia's adequacy list (which includes EEA members and Convention 108 parties) without further safeguards; otherwise under appropriate safeguards — the standard contractual clauses adopted by the Serbian

Commissioner and/or, for GDPR-scope data, the EU standard contractual clauses or an applicable adequacy framework (e.g. the EU–US Data Privacy Framework for certified US providers) — **[counsel to confirm the mechanism per subprocessor and whether any Commissioner approval or notification is required]**.

8. Return and deletion

On termination or expiry of the Contract the Processor, at the Controller's choice, deletes or returns all personal data processed on the Controller's behalf within [30] days and deletes remaining copies, unless law applicable to the Processor requires further storage. Deletion from encrypted backups occurs on the backup rotation cycle described in Annex 2. On request the Processor confirms deletion in writing.

9. Audits and information

9.1. The Processor makes available the information reasonably necessary to demonstrate compliance with Art. 45 ZZPL (Art. 28 GDPR) — descriptions of measures, relevant subprocessor certifications and audit summaries (for hyperscale subprocessors, their published certifications and audit reports, e.g. ISO 27001 / SOC 2, stand in place of on-site inspection).

9.2. The Controller may audit compliance — itself or via a mandated, confidentiality-bound auditor — at most [once per year] unless a breach or a supervisory authority requires more, with [15] days' notice, during business hours, without access to other clients' data, and at the Controller's cost.

10. Liability, law and final provisions

10.1. Liability under this DPA is subject to the limitations of the Contract, except where mandatory data-protection law provides otherwise (including Art. 86 ZZPL / Art. 82 GDPR on compensation to data subjects).

10.2. This DPA is governed by the law of the Republic of Serbia; forum as in the Contract. If this DPA conflicts with the Contract on personal-data matters, this DPA prevails.

10.3. Executed in Serbian and English; **the Serbian version prevails.**

Annex 1 — Description of processing *(completed per engagement)*

Item	Description
Categories of data subjects	End users of the Client's AI assistant / web application; the Client's staff (contact persons); individuals appearing in publicly available web content the Client instructs the Processor to collect
Types of personal data	Chat questions and answers as entered by end users (free text — content depends on what users type); pseudonymised network identifiers (IP address stored only as a salted cryptographic hash); technical logs (timestamps, latency, status); contact data of Client staff; personal data appearing in collected public web content [specify per engagement]
Special categories	None intended. End users may type special-category data into free-text fields; the assistant's configuration discourages this and the Client's end-user notice addresses it. [Adjust per engagement]

Item	Description
Processing operations	Collection, storage, retrieval (including vector search), analysis, logging, transmission to AI inference providers, deletion
Retention	Chat logs: for the Contract term unless the Controller instructs a shorter period [default: until instruction]; collected web corpora: until replaced or the Contract ends; backups: per Annex 2 rotation

Annex 2 — Technical and organisational measures (summary)

- EU-region hosting (Microsoft Azure, currently Sweden Central) for storage, database and vector search; managed PaaS services with provider-side physical security (ISO 27001, SOC 2 certified data centres).
- Encryption in transit (TLS) for all service traffic and provider APIs; encryption at rest on all storage and database services.
- Access control: role-based database roles separated per environment; application secrets held in a secrets manager (GitHub Actions secrets / Azure), never in code or logs; least-privilege deployment identities (OIDC federation, no long-lived deployment keys).
- Pseudonymisation: end-user IP addresses stored only as salted hashes; no advertising identifiers or tracking cookies in the platform default.
- Network restrictions on the database (firewall allow-listing); public endpoints rate-limited (burst / sustained / daily caps) with global budget cut-offs.
- Logging and monitoring: central log analytics and application insights with [30]-day operational retention; cost and failure alerting to a monitored mailbox.
- Development discipline: all infrastructure and configuration changes via version-controlled pull requests with automated validation; no manual production changes.
- Backups: managed automated backups of the database service per provider configuration [retention: default 7 days — adjust if agreed otherwise].

Annex 3 — Authorised subprocessors

Subprocessor	Role	Location of processing	Transfer safeguard
Microsoft (Azure)	Cloud hosting: web apps, PostgreSQL, storage, embeddings (Azure AI Foundry), e-mail/communication services, monitoring	EU (Sweden Central; some services West Europe)	EU processing; Microsoft Products and Services DPA incl. SCCs
Anthropic	Large-language-model inference for AI assistants (API; no training on submitted content per its commercial terms)	United States	[EU–US Data Privacy Framework certification and/or SCCs + Serbian SCC equivalent — counsel to confirm]
GitHub (Microsoft)	Source-code hosting and CI/CD for the Client's configured services; operational secrets storage	EU / United States	Microsoft/GitHub DPA incl. SCCs — [counsel to confirm]

Subprocessor	Role	Location of processing	Transfer safeguard
[Hetzner Online GmbH]	[Planned: auxiliary compute for scheduled data-collection jobs — added on activation per clause 7.1]	Germany (EU)	EU processing

Document: zigg_doc_dpa · Innovatica internal draft. Version and date on the cover. Changes to this document follow the repository changelog discipline.