Data Processing Agreement

Last updated: 2026-07-15 · **Effective:** 2026-07-15 · **Version:** 2026-07-15

This Data Processing Agreement ("DPA") forms part of the agreement between **Open Kinetix d.o.o.** ("Open Kinetix", the "Processor"), a company registered in the Republic of Serbia with its registered address at Kazimira Veljkovica 45, 34000 Kragujevac, Serbia, and the customer organisation subscribing to Archivez (the "Customer", the "Controller") — together the "parties". It reflects the parties' obligations under Article 28(3) of Regulation (EU) 2016/679 (the "GDPR") with respect to the processing of personal data by Open Kinetix on behalf of the Customer through the Archivez service.

This DPA is accepted electronically by a Customer administrator on behalf of the Customer at workspace onboarding (see Section 16), or executed as a countersigned document for negotiated agreements. It supplements the Terms of Service; the Privacy Policy describes Open Kinetix's processing as a controller in its own right (e.g., billing and account records).

1. Parties and roles

For personal data contained in content the Customer or its users submit to Archivez — uploaded documents, connected mailbox content, and derived chat history ("Customer Data") — the Customer is the **controller** and Open Kinetix is the **processor**. Where a Customer itself acts as a processor for a third-party controller, the Customer warrants that its instructions to Open Kinetix are consistent with its own obligations to that controller, and Open Kinetix acts as a sub-processor.

2. Definitions

"Personal data", "processing", "data subject", "personal data breach", "supervisory authority" and related terms have the meanings given in the GDPR. "Sub-processor" means a third party

engaged by Open Kinetix to process Customer Data on the Customer's behalf.

3. Subject matter, duration, nature and purpose of processing

- **Subject matter:** provision of Archivez, an AI-assisted information retrieval and conversation service over the Customer's own connected content, as described in the Terms of Service.
- **Duration:** the term of the Customer's agreement with Open Kinetix, plus the deletion period in Section 11.
- **Nature:** storage, indexing, text extraction, embedding, retrieval, and AI-model inference over Customer Data; hosting; backup; support.
- **Purpose:** solely to provide, secure, and support the service for the Customer. Open Kinetix does not use Customer Data to train AI models, for advertising, or for any purpose of its own.

4. Types of personal data and categories of data subjects

Described in **Annex 1**. Because the Customer controls what content is uploaded or connected, the actual categories depend on the Customer's use; the Customer is responsible for ensuring it has a lawful basis for the personal data it submits.

5. Processing on documented instructions

Open Kinetix processes Customer Data only on the Customer's documented instructions, including with regard to transfers to a third country, unless required to do so by Union or Member State law to which Open Kinetix is subject — in which case Open Kinetix informs the Customer of that legal requirement before processing, unless the law prohibits it on important grounds of public interest. The Customer's instructions are: this DPA, the Terms of Service, the Customer's configuration of the service, and the ordinary use of its documented features. Open Kinetix will immediately inform the Customer if, in its opinion, an instruction infringes the GDPR or other applicable data protection provisions.

6. Confidentiality

Open Kinetix ensures that persons authorised to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and access Customer Data only to the extent required to provide and support the service.

7. Security of processing (Article 32)

Open Kinetix implements and maintains appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in **Annex 2**. These include encryption of Customer Data at rest and in transit, strict per-tenant isolation at the application and query layers, role-based access control, EU-only hosting, and security logging. Open Kinetix may update these measures from time to time, provided the updates do not materially reduce the overall level of protection.

8. Sub-processors

- The Customer grants Open Kinetix **general authorisation** to engage the sub-processors listed in **Annex 3**.
- Open Kinetix will notify tenant administrators of any intended addition or replacement of a sub-processor **at least 30 days in advance**, giving the Customer the opportunity to **object on reasonable data-protection grounds**. If the parties cannot resolve an objection in good faith, the Customer may terminate the affected service and Section 11 applies.
- Open Kinetix imposes on each sub-processor, by way of contract, data protection obligations providing materially the same level of protection as this DPA, and remains fully liable to the Customer for the performance of each sub-processor's obligations.

9. Assistance with data subject requests

Taking into account the nature of the processing, Open Kinetix assists the Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to data subject requests under Chapter III of the GDPR (access, rectification, erasure, restriction, portability, objection). In the first instance this

assistance takes the form of the service's built-in tools — search, export, document and mailbox-data deletion, and account management. If a data subject request is made directly to Open Kinetix and identifies the Customer, Open Kinetix will promptly forward it to the Customer and not respond on the merits without the Customer's instruction, unless legally required.

10. Personal data breach notification

Open Kinetix notifies the Customer **without undue delay, and in any event within 72 hours**, after becoming aware of a personal data breach affecting Customer Data. The notification describes, to the extent then known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its effects, and is supplemented as further information becomes available. Open Kinetix provides reasonable assistance with the Customer's obligations under Articles 33 and 34 of the GDPR. Notification of, or response to, a breach is not an acknowledgement of fault or liability.

11. Deletion or return of data

- During the term, the Customer can delete Customer Data at any time using the service's built-in deletion features (document deletion, mailbox-data removal, account closure), and can export its content in commonly used formats. When a user disconnects a connected mailbox or un-indexes a sender, the derived indexed content is deleted **within 24 hours**.
- Upon termination of the agreement, Open Kinetix **deletes all Customer Data within 30 days**, unless Union or Member State law requires further storage. At the Customer's written request made before the end of that period, Open Kinetix will first provide a reasonable export of the Customer's stored content.
- Exceptions: security and audit logs are retained for up to 2 years, and billing records for up to 10 years, where and for as long as required by applicable law (including the Serbian Law on Accounting); deleted documents may persist in an internal soft-deleted state for up to 7 days before final erasure as part of the deletion pipeline. Data retained under these exceptions remains protected under this DPA and is not otherwise processed.

12. Audit rights

Open Kinetix makes available to the Customer information reasonably necessary to demonstrate compliance with the obligations of Article 28 GDPR, and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer. Audits are satisfied in the first instance by written responses, documentation, and available third-party attestations or certification reports. Where these are insufficient, the Customer may conduct an audit **no more than once per 12 months** (except following a personal data breach or at the instruction of a supervisory authority), on **at least 30 days' written notice**, during business hours, subject to reasonable confidentiality and security requirements, without access to other customers' data, and at the Customer's own cost.

13. International transfers

Customer Data is hosted and processed in the **European Union** (primary region `eu-central-1`, Frankfurt; AI-model inference routed through the AWS Bedrock EU cross-region inference profile, which AWS guarantees stays within EU data-residency boundaries). Open Kinetix does not transfer Customer Data outside the EU/EEA in the course of normal operations. Should any processing require a transfer to a third country not covered by an adequacy decision, the parties will rely on an appropriate safeguard under Chapter V of the GDPR — in particular the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914), which are deemed incorporated into this DPA with Open Kinetix acting under Module Two or Module Three as applicable — before the transfer takes place. Gmail API access, where the Customer's users connect Gmail, operates under each user's own Google OAuth consent and Google's data processing terms.

14. Liability

Each party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability set out in the agreement between the parties (including the Terms of Service, where no separate agreement applies). Nothing in this DPA limits either party's liability with respect to a data subject's rights under the GDPR.

15. Term, precedence and governing law

This DPA takes effect upon acceptance and remains in force for as long as Open Kinetix processes Customer Data on the Customer's behalf. In the event of a conflict between this DPA and any other agreement between the parties regarding the processing of personal data, this DPA prevails to the extent of the conflict. This DPA is governed by the same law and jurisdiction as the Terms of Service (the laws of the Republic of Serbia), without prejudice to mandatory rights and obligations arising directly under the GDPR.

16. Acceptance and versioning

- **Click-to-accept:** a Customer administrator accepts this DPA on behalf of the Customer inside the Archivez application. Open Kinetix records the accepting tenant, the accepting user's identity and role, the DPA version, the timestamp, and the network address from which acceptance was made, and makes the accepted version available to the Customer for download at any time.
- **Signed copy:** for negotiated agreements, this DPA may instead be executed as a countersigned document (a PDF copy is available here); Open Kinetix records the executed acceptance against the Customer's tenant.
- **Versions:** each version of this DPA is identified by its effective date. Material changes — including the addition of a sub-processor — are notified to tenant administrators at least 30 days in advance per Section 8 and, where required, re-accepted. Earlier versions remain available on request at privacy@archivez.io.

Annex 1 — Description of the processing

Categories of data subjects: the Customer's employees, contractors, and other authorised users of its Archivez workspace; correspondents and third parties appearing in content the Customer submits (e.g., senders, recipients, and persons mentioned in emails and documents).

Categories of personal data: identification and contact data (names, email addresses, signatures); employment and professional data; the contents of documents and email messages the Customer chooses to upload or connect, which may include any category of

personal data the Customer's content happens to contain; user account data (name, email, locale, role); usage and security metadata (timestamps, network addresses, device identifiers).

Special categories: the service is not designed or intended for special categories of personal data (Article 9 GDPR); the Customer is responsible for the content it submits and should not submit special-category data unless it has a lawful basis to process it.

Processing operations: collection (upload / mailbox synchronisation), storage, text extraction, chunking and embedding, indexing, retrieval, AI-model inference to generate answers with citations, display to authorised users, backup, deletion.

Annex 2 — Technical and organisational measures

- **Encryption at rest:** document storage in private S3 buckets with AWS server-side encryption (SSE-S3, AES-256); the application database (PostgreSQL on AWS RDS) encrypted at rest with AES-256 using AWS RDS-managed encryption; mailbox OAuth credentials additionally envelope-encrypted with AWS KMS (a distinct data-encryption key per connection, wrapped by a KMS-managed master key).
- **Encryption in transit:** TLS 1.2 or higher for all connections.
- **Tenant isolation:** every database row is scoped by tenant; the boundary is enforced at both the application and query layers.
- **Access control:** role-based access control inside the service; least-privilege, individually attributed staff access to production systems; multi-factor authentication for administrative access.
- **Hosting:** EU-only (primary region `eu-central-1`, Frankfurt); AI inference constrained to EU data-residency boundaries via the AWS Bedrock EU cross-region inference profile.
- **Logging and monitoring:** centralised security and audit logging (API activity, threat detection, access logs), error monitoring in the EU region.
- **Data lifecycle:** built-in deletion features for documents, mailbox data, and whole tenants; automated purge pipelines; backups encrypted and subject to the same retention discipline.
- **Organisational measures:** confidentiality obligations for personnel, documented information-security policies, vendor risk management with data-processing agreements in place for sub-processors, incident response procedures.

Annex 3 — Approved sub-processors

Sub-processor	Purpose	Location / routing
Amazon Web Services, Inc.	Primary cloud infrastructure (compute, storage, databases, AI inference via Bedrock)	EU — `eu-central-1` primary; EU CRI for Bedrock
Anthropic, via AWS Bedrock	Large language model inference (Claude family)	EU-only routing via Bedrock EU CRI
Cohere, via AWS Bedrock	Multilingual embedding model	EU region
Google LLC	Gmail API access (only if the Customer's users connect Gmail)	Data is pulled from the user's Google account under the user's OAuth consent
Functional Software, Inc. (Sentry)	Application crash diagnostics and error tracking	Sentry EU region (Frankfurt, Germany) — `de.sentry.io`

The current list is also available on request at privacy@archivez.io. Changes to this list follow the notification and objection process in Section 8.

Contact

- **Privacy and DPA matters:** privacy@archivez.io
- **Legal entity:** Open Kinetix d.o.o., Kazimira Veljkovica 45, 34000 Kragujevac, Republic of Serbia

Security

Data Processing Agreement

abuse@archivez.io

No analytics. No trackers. No cookies.