Data Processing Agreement

Version 1.4 · 12 November 2026

1. Parties

This Data Processing Agreement ("DPA") forms part of the agreement between ARKHOST LLC, a company registered in Armenia under TIN 02947817, with registered address at Movses Khorenatsi St., 26A, office 210, 0010 Yerevan, Armenia ("ArkHost"), and the customer identified in the ArkHost account that accepts this DPA ("Client").

The Client acts as controller for the personal data it entrusts to the services. Where the Client acts as processor for another controller, ArkHost acts as its subprocessor, and the Client is responsible for obtaining the necessary authority and giving lawful instructions. References to the Controller include the Client in that capacity where appropriate.

2. Definitions

"Personal Data", "Processing", "Controller", "Processor", "Personal Data Breach" and "Supervisory Authority" have the meanings given in Regulation (EU) 2016/679 ("GDPR"). A "Subprocessor" is a third party engaged to process Personal Data on the Controller's behalf in providing the services.

"Hosted Data" means Personal Data stored, transmitted or otherwise processed on the Client's behalf through the services, including associated content and technical data. ArkHost's own account, billing and commercial records are addressed separately in section 9.

3. Subject matter and processing scope

This DPA applies to on-behalf processing necessary to provide shared and CMS web hosting, hosted email, VPS capacity, associated DNS/CDN services, backups and technical support, and optional AI-assisted website creation or editing when used by the Client.

Processing includes storage, transmission, retrieval, delivery, organisation, security analysis, backup, recovery and deletion for the service selected by the Client. Its duration is the service term and the return, deletion and restricted backup handling described in section 9.

The Client determines what content it hosts and is responsible for its lawful collection, its notices to data subjects and the lawfulness of its instructions. It must configure and secure applications and VPS systems within its control. ArkHost does not intentionally request special-category Personal Data; the Client remains responsible for the additional safeguards required if its content includes such data.

Domain registration, certificate issuance, licence administration, payment processing and ArkHost's own customer-account operations may involve separate controller or service-specific roles. A supplier of locally installed software is not, merely by supplying that software, a recipient of all Hosted Data. The applicable privacy notices and service-specific arrangements govern those separate flows.

4. Data and data subjects

Depending on the selected service and the Client's content, processing may concern:

- names, contact details, account identifiers and technical identifiers, including IP addresses and logs;
- website files, databases and other content stored in a hosting account or VPS;
- email content, message metadata, calendars, contacts and mailbox information;
- information supplied for technical support; and

- prompts, conversation context, project files and tool results included in an optional AI request.

Data subjects may include the Client's personnel, customers, users, website visitors, correspondents and support requesters, and individuals whose data the Client includes in its content.

5. Obligations of ArkHost

ArkHost shall:

a) process Hosted Data only on documented instructions from the Controller, including the selected service and its configuration, unless Union or Member State law requires processing; in that case ArkHost shall inform the Controller before processing unless that law prohibits notification;

b) ensure that authorised persons are subject to confidentiality obligations and receive access only as needed for their duties;

c) implement appropriate technical and organisational measures, taking account of the nature, scope and risks of the processing;

d) assist the Controller, taking account of the nature of the processing, with requests to exercise data-subject rights;

e) assist with the Controller's obligations under Articles 32 to 36 GDPR, including breach response, impact assessments and prior consultation, taking account of the information available to ArkHost;

f) return or delete Hosted Data at the Controller's choice as described in section 9;

g) make available information necessary to demonstrate compliance with Article 28 GDPR and allow and contribute to audits under section 5bis; and

h) inform the Controller if, in ArkHost's opinion, an instruction infringes applicable data-protection law. ArkHost may suspend the affected instruction while it is clarified.

Acceptance of this DPA does not authorise processing outside these instructions or replace a transfer safeguard required by law.

5bis. Audit rights

The Controller may audit compliance through a written information request or an independent auditor subject to appropriate confidentiality and protection of other customers' information.

Ordinarily, an on-site audit requires at least 30 days' written notice, takes place during normal business hours and must not unreasonably disrupt services. The Controller bears its own costs and reimburses reasonable, agreed on-site assistance expenses. These arrangements must not prevent the exercise of mandatory audit rights.

Audits are ordinarily limited to once per calendar year. Additional or shorter-notice audits are permitted where required by a Supervisory Authority, following a Personal Data Breach, or where a specific, justified data-protection concern cannot reasonably be addressed otherwise. A recent independent report or questionnaire may provide sufficient evidence, but does not exclude a justified inspection or a mandatory right.

6. Security measures

Measures appropriate to the selected service include protected administrative access, access restrictions, TLS for supported management/web/mail connections, network firewalls, service isolation, security updates, logging and backup arrangements. Imunify360 malware scanning, WAF and related protection apply to the web-hosting services on which they are installed. Suspicious files and relevant security information may be submitted for remote analysis as part of that protection.

Backup facilities, restore options and application responsibilities depend on the service. Separate offsite storage is used for the applicable hosting and mail backups. The Client is responsible for the security and TLS configuration of applications and VPS systems within its control. Included backup and recovery features are described with the selected service.

ArkHost shall review its measures as risks and services change. The Client may request relevant security information, subject to confidentiality and the protection of other customers.

7. Subprocessors and other recipients

The Controller grants general authorisation to use the subprocessors relevant to its selected services. ArkHost shall impose the relevant data-protection obligations in a written arrangement with each Subprocessor and remains responsible to the Controller for the performance of those obligations.

The **Confidential Subprocessor Schedule** forms part of this DPA. It identifies the suppliers relevant to each service, their identities and contact details, the processing entrusted to them, locations and applicable onward-processing information. It is supplied with the full DPA document in the authenticated client document area before acceptance and remains available during the relationship. Access does not depend on having already accepted this version. A prospective contracting customer may obtain access before authorising processing.

The schedule is maintained separately from this public agreement. Additions and replacements follow the notice and objection procedure below; a schedule update alone does not require a new version of the general DPA. Previous schedule versions and acceptance records are retained. Reasonable commercial-confidentiality obligations do not prevent disclosures needed to fulfil data-protection duties, obtain authorised professional advice or cooperate with Supervisory Authorities.

The optional AI chain receives the prompts and project context included when that feature is used, not every hosted website by default. AI processing is not covered by a blanket EU-only processing promise. The Client must have authority to include third-party Personal Data in a request. Feature-specific recipients and processing information are addressed separately in the confidential schedule; use of the feature does not waive GDPR requirements.

Merchant-of-Record, registrar, licence-validation and authorised software-support disclosures are assessed under their actual roles and the applicable service-specific arrangements. ArkHost's Privacy Policy addresses its own controller records.

ArkHost shall notify the Controller by email to its registered account address at least 14 days before an intended addition or replacement of a Subprocessor. The Controller may object within that period on reasonable data-protection grounds. The parties shall seek a reasonable solution; if the objection cannot reasonably be accommodated, the Controller may terminate the affected services without penalty. Fees for services already provided and unaffected services remain payable. Further processing-chain details may be requested at privacy@arkhost.com.

8. Personal Data Breaches

ArkHost shall notify the Controller without undue delay after becoming aware of a Personal Data Breach affecting Hosted Data, and in any event within 48 hours. This is an outer limit for initial notification, not permission to delay.

Notification shall include, as information becomes available, the nature of the breach, affected data and data subjects, likely consequences, mitigation and a contact point. Information may be provided in phases without undue further delay. ArkHost shall cooperate with the Controller's investigation and notification obligations, including Article 33 GDPR.

9. Return, deletion and retention

a) At termination, the Controller may choose return or deletion of Hosted Data. The Controller may communicate its choice before termination or within 30 days afterwards. A request concerning remaining copies shall be handled without undue delay; this does not require recreating data already deleted on the Controller's documented instructions. Return uses the export facilities or a suitable format available for the selected service. Once return is completed, remaining copies shall be deleted unless applicable law requires their storage. Return or deletion is not conditional on payment of outstanding fees.

b) The three-year account-record and seven-year invoice retention periods in ArkHost's Privacy Policy concern ArkHost's own controller business records. They do not authorise retaining all Hosted Data for those periods or override the Controller's return/deletion choice.

c) Any requirement under Union or Member State law to retain processor-held Hosted Data must be limited to the applicable requirement, with access restricted, notification unless legally prohibited, and deletion when that requirement ends. A third-country disclosure demand is subject to the legal and transfer assessment in section 10, not a general authorisation to disclose.

d) Deletion instructions also apply to backup copies. Copies temporarily retained for recovery must be restricted from ordinary processing and securely deleted through the applicable backup rotation. Deletion instructions shall be reapplied if a backup is restored. ArkHost shall provide the relevant service-specific retention information on request. The controller-record periods in paragraph b) do not extend backup retention for Hosted Data.

10. International processing and transfers

ArkHost is established in Armenia and administers services from Armenia. Core hosting, mail and VPS infrastructure is in the EU, but EU storage is distinct from remote administrative access and from security or optional AI processing outside the EEA. A supplier's registered address does not establish every processing location.

Hosted Data shall be transferred or made accessible internationally only on documented instructions and subject to applicable data-protection requirements. Where a restricted transfer requires a safeguard, the parties shall use the applicable Standard Contractual Clauses or another lawful mechanism, with the required assessment and supplementary measures. Acceptance of this DPA alone is not an adequacy decision or a substitute for such a mechanism.

ArkHost shall provide relevant information about recipients, locations and safeguards on request. It shall assess legally binding disclosure demands, notify the Controller unless prohibited, and challenge an unlawful demand where required. Mandatory transfer terms and data-subject rights take precedence over conflicting service terms.

11. Duration, versions and acceptance

This DPA applies from acceptance of version 1.4 and continues for the service term and for any remaining on-behalf processing until return or deletion. Confidentiality and other obligations that must survive termination remain applicable. Existing records of acceptance of earlier versions are preserved; they are not treated as acceptance of this version.

12. Contact

Data-protection contact: **privacy@arkhost.com**.

ARKHOST LLC, Movses Khorenatsi St., 26A, office 210, 0010 Yerevan, Armenia.

13. Governing law and precedence

Armenian law governs this DPA and the courts of Yerevan have jurisdiction, subject to mandatory consumer, data-protection, jurisdiction and data-subject rights. This DPA prevails over conflicting general service terms for on-behalf processing. Applicable mandatory law and any binding transfer clauses prevail over conflicting provisions of this DPA.