Data Processing Agreement

For customer content routed through Wakemark, the customer is the controller and Wakemark is the processor (GDPR Article 28). This agreement sets out the processor terms — instructions, security, sub-processors, data-subject assistance, breach notice, deletion — and the transfer safeguards for processing outside the EEA/UK.

Last updated: 2026-07-13

HOW THIS DPA APPLIES TODAY

This DPA is incorporated into the Terms of Service and applies automatically, without a signature, to the extent customer content includes personal data — including on the free service. No paid or enterprise agreements are in operation yet (nothing is charged today); a countersigned copy of this DPA, which some organisations require for their records, will be available on entering a commercial agreement.

1. Roles and structure

This DPA forms part of the Terms of Service and applies to the extent customer content includes personal data.

- For customer content — prompts, parameters, generated media, the job/event ledger, provenance sidecars, lineage, and the BYOK credentials in Wakemark's custody — the customer is the controller and Wakemark is the processor, acting only on documented instructions.
- Where the customer is itself a processor for a third-party controller, Wakemark acts as the customer's sub-processor; the customer warrants its instructions to Wakemark are authorised by that controller.
- For account and workspace data, Wakemark is an independent controller, governed by the Privacy Policy — not by this DPA.
- The contracting processor is O ÷W¦† â ±1r, an individual (a natural person) based in Türkiye, operating the Wakemark service.

2. Details of processing (Annex I)

Subject matter & duration

Customer content processed through the Wakemark control plane, for the term of the Agreement plus the deletion process in section 10.

Nature & purpose

Routing generation requests to the providers the customer connects; taking byte-exact custody of outputs in platform storage or the customer's own bucket; detecting and logging C2PA provenance; recording an append-only audit ledger and lineage graph; executing the customer's retention policy; serving verification and audit exports; encrypted custody of BYOK credentials.

Categories of data subjects
Determined by the customer — typically the customer's personnel and end users, and individuals appearing in or identifiable from prompts, reference inputs, or generated media.

Categories of personal data
Whatever personal data the customer's prompts, inputs, and generated media contain, plus the ledger entries that record them (including raw provider responses, which can embed inputs or outputs) and provenance metadata.

Special categories
The service is not designed for special-category data. The customer must not submit it unless the customer has a lawful basis and appropriate safeguards; any such data is processed only as part of customer content under this DPA.

3. Instructions

The customer's documented instructions are: this DPA and the Agreement; the API calls and dashboard actions the customer takes (job submissions, routing policy, storage-connection choices); the per-project retention policy and per-job overrides; and deletion/export requests. Wakemark processes customer content only per those instructions, and will inform the customer if, in its view, an instruction infringes the GDPR (to the extent legally able to do so). Routing a job to a provider the customer connected, and writing to a bucket the customer connected, are instructed transmissions — see section 6.

4. Confidentiality

Persons authorised to process customer content are bound by confidentiality obligations. Wakemark is currently operated by its founder; access to production systems is correspondingly narrow, and this clause binds any future personnel before access is granted.

5. Security measures (Annex II summary)

Wakemark implements the technical and organisational measures summarised below and described on Security & Trust; these constitute the Annex II measures of the Standard Contractual Clauses referenced in section 12.

- Credential custody: per-secret envelope encryption (AES-256-GCM data keys wrapped by a managed key-management service), with the tenant and purpose bound into both the ciphertext's authenticated data and the KMS encryption context — ciphertext moved to another tenant's row fails to decrypt at two independent layers. Plaintext exists only in memory at job submission; never in logs or errors.
- Tenant isolation: every tenant-scoped query carries the tenant; handlers compile only against tenant-scoped store facades, and a query-log assertion verifies the predicate on both database backends.
- Integrity & auditability: an append-only event ledger; byte-exact custody with sha256 digests recorded at write time; content redactions are themselves ledgered events.
- Storage: private buckets; reads via short-lived signed URLs; media never made public.
- Erasure: the deletion flow of section 10, verified by automated seed-and-search tests on both database backends.
- No certifications are held or claimed today (SOC 2 is groundwork, not an attestation).

6. Sub-processors

The customer grants general written authorisation for the categories of sub-processor at /legal/subprocessors — cloud object storage, managed database, key management, application/compute hosting, authentication, transactional email, and web hosting/analytics. A current itemized list naming the specific sub-processors is available to the customer on request. Wakemark will: give at least 30 days' notice before a new or replaced sub-processor begins processing customer content, allowing the customer to object on reasonable data-protection grounds (and, if the objection cannot be resolved, to terminate the affected service); impose data-protection obligations materially equivalent to this DPA on each sub-processor; and remain responsible for their performance.

NOT SUB-PROCESSORS: THE SERVICES YOU CONNECT

The generation providers you connect with your own key, and the vendor of a storage bucket you connect, are engaged by YOU, on your account and your terms — they are independent processors (or controllers) in your own chain, not Wakemark sub-processors. Wakemark transmits customer content to them solely on your documented instruction. No billing vendor processes customer data in this build; if billing launches, the responsible provider is engaged with notice first.

7. Data-subject requests

Wakemark will promptly redirect to the customer any data-subject request it receives concerning customer content, and will assist the customer in fulfilling requests — primarily through the self-service surface: the account export (access/portability), per-project retention and per-job overrides (erasure/restriction of content), asset-level records and the verifier (information), and account deletion. Wakemark does not respond directly to a data subject on the customer's behalf except on the customer's instruction or where the law requires.

8. Assistance (Articles 32–36)

Taking into account the nature of the processing and the information available to it, Wakemark will assist the customer with security of processing, breach notification, data-protection impact assessments, and prior consultation — including by providing the documentation in section 11.

9. Personal-data breach

Wakemark will notify the customer without undue delay after becoming aware of a personal-data breach affecting customer content, and will provide the information reasonably available to it — the nature of the breach, the categories and approximate volumes concerned, the likely consequences, and the measures taken or proposed — supplementing as investigation continues. The customer remains responsible for its own notification obligations to authorities and data subjects.

10. Deletion and return

- Return (self-service, any time): the full account export — ledger, job history, custody records, lineage — is downloadable from the dashboard, including during a deletion grace period. Bytes in the customer's own bucket are already in the customer's hands.

- Deletion during the term: the customer's retention policy is the standing deletion instruction, executed per project and per job; content-bearing ledger fields are redacted to an auditable tombstone.
- Deletion on termination: the account-deletion flow — immediate purge of provider credentials and key revocation at request time; a 30-day frozen grace period (export/cancel only); then a hard purge of every content store Wakemark controls, with a PII-free erasure receipt (hashed identifier + counts) and anonymized, content-free usage-metering counters (account/project references hashed the same way) as the surviving proof.
- The BYOK boundary: offboarding never touches the customer's own bucket — Wakemark deletes its credentials and references; the customer's objects stay theirs.
- Backups: sub-processor backups (e.g. database point-in-time recovery, storage versioning) are outside the application's reach and age out on the vendor's retention window — disclosed, not claimed erased.

11. Audits and information

Wakemark will make available the information necessary to demonstrate compliance with this DPA — this document, the subprocessor list, the security overview, erasure receipts for completed deletions, and the per-project audit export — and will allow and contribute to audits, including inspections, conducted by the customer or its mandated auditor at reasonable intervals, under confidentiality, with reasonable notice — no more than once in any twelve-month period (unless required by a supervisory authority or following a personal-data breach), at the customer's cost unless the audit reveals material non-compliance.

12. International transfers

Media storage, key management, the database, and compute stay in the EU. Authentication, transactional email, and web hosting process in the United States.

STANDARD CONTRACTUAL CLAUSES

For personal data transferred outside the EEA/UK, the parties incorporate the EU Standard Contractual Clauses — Module 2 (controller-to-processor), or Module 3 (processor-to-processor) where the customer is itself a processor — and the UK International Data Transfer Addendum where UK data is involved, each with the annexes completed from this DPA, the security measures in section 5, and the sub-processor list. The SCCs prevail over any conflicting term of this DPA to the extent of the conflict.

13. Liability and term

Liability under this DPA is subject to the limitations in the Terms of Service. This DPA applies for as long as Wakemark processes customer content and ends when deletion under section 10 completes.

14. Article 50 & provenance

Wakemark is designed to support Article 50 workflows through provenance preservation, detection, logging, verification, and the audit export — described precisely, with its limits, in the Article 50 addendum. Neither the service nor this DPA ensures or guarantees the customer's regulatory compliance; the controller remains responsible for its own obligations.