Data Processing Agreement (DPA)

GDPR Article 28 data processing agreement template · version 2026.06.10-v3 · last updated 2026-06-10

Preamble

This Data Processing Agreement ("DPA") sets out, in application of Article 28 of Regulation (EU) 2016/679 ("GDPR"), the conditions under which the publisher of the Scope service processes personal data on behalf of the Customer Organisation. It complements and forms an integral part of the Terms of Service. In the event of any conflict between this DPA and the Terms of Service, this DPA prevails for any matter relating to data protection.

Parties

Processor : Amir KELLOUSIDHOUM, sole trader (entrepreneur individuel) — 133 rue du Général de Gaulle, 94350 Villiers-sur-Marne, France · SIRET 917 709 024 00017 ("Scope").

Controller : {{client_company_name}}, {{client_legal_form}}, registered under number {{client_registration_number}}, with registered office at {{client_registered_address}}, represented by {{client_signatory_name}} acting as {{client_signatory_title}} ("Customer").

Point of contact : DPO / data protection contact — dpo@getscope.dev. Incident notification: security@getscope.dev (handled within 72 hours after becoming aware of the breach).

Article 1 — Subject matter and duration

Scope processes the Customer Data for the sole purpose of providing the Service defined in the Terms of Service. The duration of the processing matches the term of the subscription, extended by the deletion period set out in Article 8.

Article 2 — Nature and purpose of the processing

The processing consists of ingesting, structuring, transforming (via third-party AI subject to a no-training clause), storing, displaying, exporting and signing the scoping documents produced from the Content provided by the Customer. The purpose is strictly operational: to execute the AI pipeline and to enable the Customer to produce and share its deliverables.

Article 3 — Categories of personal data

- Professional identification data of the Customer's staff and of the contacts mentioned in the briefs.
- Free-form professional content: text, transcribed audio, PDFs, notes.
- Technical metadata: timestamps, file name, file size, connection IP address.

No special categories of data within the meaning of Article 9 GDPR (health, religion, orientation, etc.) and no data relating to criminal convictions (Article 10) are expected. The Customer undertakes not to upload such data to the Service.

Article 4 — Categories of data subjects

- Staff and authorised users of the Customer.
- End-clients of the Customer and their representatives mentioned in briefs, scoping notes or proposals.
- Signatories of documents submitted to electronic signature.

Article 5 — Obligations of the Processor

- Process the Data only on documented instructions from the Customer (the acceptance of the Terms of Service constitutes such instructions, save for any specific instruction sent in writing to dpo@getscope.dev).

- Ensure that persons authorised to process the Data are subject to a contractual or statutory duty of confidentiality.
- Implement the technical and organisational measures described in Annex 2 (Article 32 GDPR).
- Engage no sub-processor without prior information of the Customer under the conditions of Article 6 (see also Annex 3).
- Assist the Customer in responding to requests for the exercise of data subjects' rights (Articles 12 to 22 GDPR).
- Notify the Customer of any personal data breach within seventy-two (72) hours of becoming aware of it (Article 33.2 GDPR).
- At the Customer's choice, delete or return the Data at the end of the engagement (Article 8 below).
- Make available to the Customer all information necessary to demonstrate compliance with the obligations of Article 28 GDPR and to allow audits, including inspections (Article 9 below).

Article 6 — Sub-processors

The Customer authorises Scope to engage the sub-processors listed in Annex 3. Any change to that list (addition or replacement) is notified by email to subscribed customers at least thirty (30) days before it takes effect, in application of Article 28.2 GDPR. The Customer may object to a new sub-processor on legitimate grounds related to data protection; in the absence of agreement, the Customer may terminate the subscription without penalty before the change takes effect.

Article 7 — Transfers outside the European Union

Customer Data is stored within the European Union. However, certain processing operations may involve a transfer to a third country, governed by the Standard Contractual Clauses adopted by the European Commission (Implementing Decision (EU) 2021/914 of 4 June 2021), incorporated by reference into the contracts with each sub-processor, and supplemented by the additional measures described in Annex 2.

Article 8 — Fate of the Data at the end of the contract

Upon termination of the subscription, the Customer may, for thirty (30) days, export its scoping documents and its Content using the tools provided by the Service. At the end of that period, Scope deletes all the Data within a maximum of thirty (30) additional days, save for legal retention obligations (for example, accounting records, retained for ten (10) years pursuant to Article L.123-22 of the French Commercial Code). A deletion certificate is available on request to dpo@getscope.dev.

Article 9 — Audit and compliance

Scope makes available to the Customer, on reasoned request, the documentation necessary to demonstrate compliance with this DPA: security policy, sub-processor registry, technical and organisational measures, register of personal data breaches. The Customer may, at its own expense and on reasonable thirty (30) days' prior notice, conduct once per year a documentary audit, or have it conducted by an independent third party bound by professional secrecy and pre-approved by Scope (such approval not to be unreasonably withheld).

Article 10 — Governing law and jurisdiction

This DPA is governed by French law. Any dispute relating to its interpretation or performance shall be submitted to the competent courts within the jurisdiction of the Tribunal Judiciaire de Créteil (94), France, subject to mandatory rules of jurisdiction.

Annex 1 — Description of the processing

Activities : Ingestion, structuring, AI-assisted generation, storage, export, sharing and electronic signature of scoping documents.

Categories of Data : Professional identifiers, free-form content, technical metadata.

Data subjects : Customer's staff, Customer's end-clients mentioned in briefs, signatories of documents submitted to electronic signature.

Duration : Term of the subscription, extended by the deletion period set out in Article 8.

Location : European Union (Dublin, Frankfurt, Paris, Netherlands), with framed transfers to the United States for certain sub-processors (see Annex 3).

Annex 2 — Technical and organisational measures

- Encryption: TLS 1.3 in transit, AES-256 at rest (Postgres volumes and Storage buckets).
- Authentication: passwords hashed and salted (bcrypt), MFA mandatory for administrator accounts.
- Multi-tenant isolation: systematic Postgres Row Level Security (RLS) policies, segregation by org_id in the database and in Storage paths ({org_id}/{project_id}/...).
- Audit logs: immutable journal of sensitive mutations (export, signature, credit debits), retained twenty-four (24) months for Enterprise accounts.
- Idempotency: every webhook (Stripe, DocuSeal) and every credit-ledger operation is replayable without side effects, identified by event_id or request_id.
- Secrets management: encrypted environment variables, rotation of API keys, segregation of user / service-role roles.
- Backups: daily automated snapshots, multi-AZ replication.
- Payment security: no card data is processed by Scope; full tokenisation by Stripe (PCI DSS Level 1).
- Incident response: notification within seventy-two (72) hours pursuant to Article 33 GDPR, documented runbook, single point of contact dpo@getscope.dev.
- Secure deletion: scheduled purge upon termination, save for accounting obligations.

Annex 3 — Sub-processors

List as of 2026-06-10, version 2026.06.10-v3. The live version is published at https://getscope.dev/trust and exposed as JSON at https://getscope.dev/api/sub-processors.json.

Railway

Legal entity : Railway Corp.

Purpose : Hosting of the Next.js application on a persistent container and execution of application routes.

Location : EU West region (European Union)

Jurisdiction : US

Certifications : SOC 2 Type II, EU Standard Contractual Clauses (SCCs)

US Cloud Act mitigation : Railway Corp. is US-domiciled. Scope deploys the application service in the EU West region and does not persist durable customer content on Railway; durable data (briefs, scoping documents, exports, audit logs) resides in Supabase EU. Railway's DPA incorporates applicable transfer mechanisms, including SCCs.

DPA : https://railway.com/legal/dpa

Supabase

Legal entity : Supabase, Inc.

Purpose : Postgres database, authentication, object storage and Realtime for briefs, scoping documents, audit log and exports.

Location : Dublin, Ireland (eu-west-1 region)

Jurisdiction : US

Certifications : SOC 2 Type II, HIPAA-ready

US Cloud Act mitigation : Supabase, Inc. is US-domiciled, but the Scope project is provisioned in the eu-west-1 (Dublin) region. Transfers outside the EU are governed by Supabase's DPA and SCCs; access is limited through RLS, separated keys and data minimization.

DPA : https://supabase.com/legal/dpa

OpenRouter

Legal entity : OpenRouter, Inc.

Purpose : LLM router with contractual data_collection=deny clause: your prompts and the generated responses are never used to train the models.

Location : Stateless proxy (United States) routing requests to OpenAI and Anthropic (United States), under EU Standard Contractual Clauses

Jurisdiction : US

Certifications : EU Standard Contractual Clauses (SCCs)

US Cloud Act mitigation : OpenRouter is a stateless proxy: no prompt or output is retained on the OpenRouter side beyond processing time. The contract enforces `data_collection=deny` downstream, which prevents downstream LLM providers from logging or training on your prompts. Today, requests are routed in practice to OpenAI (GPT-4o and GPT-4o mini, operated from the United States) and Anthropic (Claude Sonnet 4.6 and Haiku 4.5, operated from the United States): transfers are governed by the EU Standard Contractual Clauses and each provider's own DPA. An Enterprise EU-resident routing option (Anthropic Claude via AWS Bedrock Paris region, or Mistral Large hosted in Paris) is under internal validation and will be offered on request as soon as FR quality benchmarks are conclusive. When OpenRouter is unavailable (PH10, 2026-06-10), a resilience chain switches calls to Mistral AI direct (Paris, EU) then Anthropic direct (United States, EU SCCs) — both links are governed by the same no-training obligations and switchovers are audited (audit_logs, action `pipeline.llm_provider_failover`).

DPA : https://openrouter.ai/terms

Gladia

Legal entity : Gladia SAS

Purpose : Enterprise-grade audio transcription specialized in French — used for scoping notes from meeting recordings.

Location : Paris, France

Jurisdiction : EU

Certifications : GDPR, DPA available

DPA : https://www.gladia.io/compliance-hub

Mistral AI

Legal entity : Mistral AI SAS

Purpose : Text extraction by OCR (mistral-ocr-latest) on PDF and image files uploaded as brief pieces. Source content transits the Mistral API during processing; the structured markdown result is persisted to Supabase EU. Enabled only when the MISTRAL_OCR_ENABLED flag is set server-side; otherwise the PDF/image upload surface displays a "coming soon" notice and no call is emitted. Secondary

usage (PH10, 2026-06-10): LLM fallback provider in the resilience chain. If OpenRouter becomes unavailable, extraction, clarification and scoping calls switch to the Mistral API for the duration of the outage. Paris (EU) hosting — preferred over Anthropic direct (US) in the failover order to minimise data exposure. Enabled only when MISTRAL_API_KEY is configured; otherwise the link is skipped and the chain tries Anthropic direct.

Location : Paris, France

Jurisdiction : EU

Certifications : GDPR, EU sovereign hosting, No-training by default

DPA : https://mistral.ai/terms

DocuSeal (self-hosted)

Legal entity : Scope (auto-hébergé — instance DocuSeal)

Purpose : eIDAS-compliant e-signature for scoping notes, proposals and DPAs — DocuSeal instance self-hosted by the publisher on Railway (EU West region), no signed data is shared with a third party.

Location : Railway, EU West region (European Union)

Jurisdiction : EU

Certifications : eIDAS (advanced electronic signature), Self-hosted in the EU

DPA : /dpa

Resend

Legal entity : Plus Five Five, Inc. (Resend)

Purpose : Delivery of transactional emails (notifications, confirmations, magic links, signatures, exports ready).

Location : eu-west-1 region (Ireland)

Jurisdiction : US

Certifications : SOC 2 Type II, HIPAA-ready

US Cloud Act mitigation : Resend is operated by a US company. Scope uses the eu-west-1 sending region for transactional emails and limits transmitted content to what is necessary for deliverability. Resend's DPA incorporates SCCs.

DPA : https://resend.com/legal/dpa

Stripe

Legal entity : Stripe Payments Europe Ltd

Purpose : Payment processing, subscription management and customer invoice issuance. No card data ever transits Scope's servers (full tokenization).

Location : Dublin, Ireland

Jurisdiction : EU

Certifications : PCI DSS Level 1, SOC 1, SOC 2 Type II, ISO 27001

DPA : https://stripe.com/legal/dpa

Plausible

Legal entity : Plausible Insights OÜ

Purpose : Self-hosted web analytics with no cookies and no personal data. Activated only after explicit

consent.

Location : Germany (Hetzner)

Jurisdiction : EU

Certifications : GDPR by design, Cookieless

DPA : https://plausible.io/dpa

GlitchTip

Legal entity : Burke Software & Consulting LLC (GlitchTip)

Purpose : Capture of runtime errors on the server and in the browser, to identify and fix regressions. Payloads are scrubbed (PII, secrets) before transmission.

Location : DigitalOcean Frankfurt, Germany (EU data residency)

Jurisdiction : US

Certifications : EU data residency, Open source (MIT), DPA on request (contractual no-transfer commitment)

US Cloud Act mitigation : Burke Software & Consulting LLC is US-domiciled, but the GlitchTip instance used by Scope is hosted on DigitalOcean Frankfurt with a contractual EU data residency and no-transfer clause. Payloads are scrubbed SDK-side (PII, tokens, secrets) before transmission. Default retention: 30 days.

DPA : https://glitchtip.com/privacy/

Cloudflare R2 (EU)

Legal entity : Cloudflare, Inc.

Purpose : S3-compatible object storage (EU bucket) holding the weekly Postgres database backups (compressed and encrypted SQL dump). No application content is read live from this bucket — access is restricted to disaster-recovery dumps.

Location : European Union (R2 jurisdiction = EU, bucket pinned to EU)

Jurisdiction : US

Certifications : SOC 2 Type II, ISO 27001, EU Standard Contractual Clauses (SCCs), 90-day retention (bucket lifecycle policy)

US Cloud Act mitigation : Cloudflare, Inc. is US-domiciled, but the R2 bucket used by Scope is provisioned with EU jurisdiction (R2 jurisdictional restrictions option). Stored content is limited to compressed/encrypted Postgres dumps reserved for disaster-recovery; no application data is read live from this bucket. The Cloudflare DPA incorporates the SCCs. Retention is capped at 90 days by the bucket lifecycle policy.

DPA : https://www.cloudflare.com/cloudflare-customer-dpa/

Cloudflare

Legal entity : Cloudflare, Inc.

Purpose : DNS resolution for the getscope.dev domain and email routing to professional inboxes. No application data transits Cloudflare.

Location : Global anycast network

Jurisdiction : GLOBAL

Certifications : SOC 2 Type II, ISO 27001, PCI DSS

US Cloud Act mitigation : Cloudflare only processes DNS and email routing metadata. No client application data (briefs, scoping documents, exports) is exposed. The Cloudflare DPA

incorporates the EU Standard Contractual Clauses.

DPA : https://www.cloudflare.com/cloudflare-customer-dpa/

Better Stack

Legal entity : BetterStack UAB

Purpose : Uptime monitoring of getscope.dev public routes and heartbeats from scheduled jobs (crons). No personal data transits Better Stack: only public HTTP probes and job-completion pings.

Location : Vilnius, Lithuania (EU)

Jurisdiction : EU

Certifications : GDPR, EU hosting, DPA available

DPA : https://betterstack.com/privacy

Signatures

DocuSeal fields to place before sending: {{client_signature}}, {{client_signatory_name}}, {{client_signatory_title}}, {{client_signed_at}}, {{scope_signature}}, {{scope_signed_at}}. To receive a pre-filled DocuSeal envelope, write to dpo@getscope.dev with the Customer legal name, registered address, registration number and authorized signatory.