Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms part of the agreement between the Customer and Ephemera for the provision of the Ephemera Kubernetes security-audit service (the "**Service**"), and governs the Processing of Personal Data carried out by Ephemera on behalf of the Customer.

> **Draft for legal review.** This document reflects the data flows and safeguards implemented in the product as of the version below. Entity-specific details marked *like this* must be completed and the agreement executed by authorised signatories before it is relied upon. Subprocessor regions and contractual transfer mechanisms must be confirmed by legal/ops.

1. Parties & roles

1.1 Controller. The "**Customer**" identified in the order or account record (*legal name, registered address*) acts as the data **Controller** in respect of the Personal Data described in Annex I.

1.2 Processor. "**Ephemera**" (*registered legal entity, company number, registered address*) acts as the data **Processor**. Ephemera operates a multi-tenant, region-pinned platform with separate EU and US data planes.

1.3 Scope. Where the Customer is itself a processor acting on behalf of a third-party controller, Ephemera acts as a sub-processor and the obligations below apply *mutatis mutandis*.

2. Definitions

"**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Sub-processor**", "**Data Subject**", "**Supervisory Authority**" and "**Personal Data Breach**" have the meanings given in Regulation (EU) 2016/679 ("**GDPR**"). "**Applicable Data Protection Law**" means the GDPR, the UK GDPR, and any other data-protection law applicable to the Processing. "**SCCs**" means the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914.

3. Subject-matter & instructions

3.1 The subject-matter, duration, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects are described in **Annex I**.

3.2 Documented instructions. Ephemera Processes Personal Data only on the Customer's documented instructions, including with regard to international transfers, unless required to do otherwise by EU or Member-State law (in which case Ephemera informs the Customer of that

requirement before Processing, unless the law prohibits it on important grounds of public interest). This DPA, the main agreement, and the configured use of the Service constitute the Customer's complete and final instructions.

3.3 Unlawful instructions. Ephemera informs the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law.

4. Processor obligations (GDPR Art. 28(3))

4.1 Confidentiality. Ephemera ensures that persons authorised to Process the Personal Data are bound by confidentiality obligations and are subject to role-based access control (roles: `admin`, `auditor`, `team-lead`, `executive`).

4.2 Security. Ephemera implements the technical and organisational measures set out in **Annex II**, appropriate to the risk (GDPR Art. 32).

4.3 Sub-processors. The Customer grants general authorisation for the sub-processors listed in **Annex III**. Ephemera will inform the Customer of intended additions or replacements at least *30 days* in advance, giving the Customer the opportunity to object on reasonable data-protection grounds. Ephemera imposes data-protection obligations on each sub-processor that are no less protective than those in this DPA, and remains fully liable for its sub-processors' performance.

4.4 Data-subject requests. Taking into account the nature of the Processing, Ephemera assists the Customer by appropriate technical and organisational measures, insofar as possible, in responding to requests to exercise Data-Subject rights (access, rectification, erasure, restriction, portability, objection).

4.5 Assistance. Ephemera assists the Customer in ensuring compliance with the obligations in GDPR Arts. 32–36 (security, breach notification, data-protection impact assessments, prior consultation), taking into account the nature of Processing and the information available to Ephemera.

4.6 Deletion or return. On termination of the Service, and at the Customer's choice, Ephemera deletes or returns all Personal Data and deletes existing copies, unless retention is required by law. Note that **raw cluster artifacts are automatically deleted within 24 hours** of collection in the ordinary course of operation (see §6 and Annex II); aggregate scores and trends are retained for the duration of the Service unless the Customer requests deletion.

4.7 Audit & information. Ephemera makes available to the Customer all information necessary to demonstrate compliance with Art. 28 and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor it mandates, on reasonable notice and subject to confidentiality. Ephemera may satisfy this obligation by providing third-party attestations once available (see the attestation roadmap on the Trust Center) and the cryptographic deletion proof described in §6.

5. International transfers

5.1 Region pinning. Stored Personal Data does not cross a region boundary. The EU and US deployments run on separate, region-pinned control-plane databases (EU on Scaleway, US on DigitalOcean); a tenant's record — together with its cluster dumps, findings and PDFs — resides solely in that tenant's home-region database and is not replicated to the other region. The only data replicated for durability is the per-region, ed25519-signed retention log, whose disaster-recovery replica stays within the same jurisdiction.

5.2 AI processing (region-local). The AI layer of the Service calls each tenant region's LLM provider **directly, at that provider's in-region endpoint**: EU-tenant prompts are sent to Mistral AI in the EU (France); US-tenant prompts are sent to Anthropic in the US. Prompts are built from **redacted** findings text only (no secrets, no raw manifests). There is no shared cross-region request aggregator in the path: the endpoint and API key are selected from the same region entry as the model, so an EU tenant's redacted text is processed inside the EEA and is **not** transferred to a third country. Provider-side commitments on retention and on not training models on Customer data are governed by the applicable provider Data Processing Agreement (Mistral / Anthropic), to be confirmed by legal/ops; the transport residency described here is distinct from those retention guarantees.

5.3 Other transfers. Any other transfer of Personal Data to a third country is made only where an adequacy decision applies or appropriate safeguards (e.g. SCCs) are in place.

6. Retention & deletion proof

Raw artifacts (cluster dumps and intermediate scan inputs) auto-delete within 24 hours of collection. Each deletion is recorded in an append-only, ed25519-signed retention log, enabling the Customer to independently verify that a given artifact was destroyed. Aggregate, non-raw outputs (scores, trends, finding metadata) are retained to provide continuity of the Service.

7. Personal Data Breach

Ephemera notifies the Customer without undue delay, and in any event within *72 hours*, after becoming aware of a Personal Data Breach affecting the Customer's Personal Data, providing the information reasonably required for the Customer to meet its own notification obligations (GDPR Arts. 33–34).

8. Liability, term & governing law

8.1 This DPA is effective for as long as Ephemera Processes Personal Data on the Customer's behalf and survives termination until all such Personal Data is deleted or returned.

8.2 Liability under this DPA is subject to the limitations and exclusions of liability set out in the main agreement.

8.3 This DPA is governed by the law of *[governing-law jurisdiction]*. In case of conflict between this DPA and the main agreement on matters of data protection, this DPA prevails.

For the Customer (Controller)	**For Ephemera (Processor)**
Name	Name
Title	Title
Signature & date	Signature & date

Annex I — Description of Processing

A. List of parties

Controller / data exporter: the Customer (*legal name, address, contact*).
Processor / data importer: Ephemera (*legal entity, address, DPO/security contact: security@ephemera.sh*).

B. Categories of Data Subjects

- The Customer's authorised users of the Service (account holders / dashboard users).
- Individuals whose Personal Data may incidentally appear in collected Kubernetes cluster configuration despite redaction (e.g. email addresses in annotations). Ephemera redacts secrets and known sensitive fields at collection time; cluster data is not intended to contain Personal Data.

C. Categories of Personal Data

Category	Examples
Account & identity	User name, email address, hashed credentials, role assignment, tenant/billing email
Billing	Billing contact (company name, billing email). Any payment processor engaged for paid plans acts as Ephemera's processor for billing data for which Ephemera is the controller — it does not Process Customer Personal Data under this DPA and is disclosed in Ephemera's privacy notice rather than in Annex III.
Operational metadata	Authentication events, request metadata, error/stack traces (no cluster data)
Cluster-derived (incidental)	Redacted Kubernetes configuration; secrets and known sensitive fields removed at collection

No special-category data (GDPR Art. 9) is intended to be Processed. The Customer must not submit special-category data through the Service.

D. Nature & purpose of Processing

Collection of Kubernetes cluster state; offline security scanning; deduplication and fusion of findings; compliance mapping; generation of reports (PDF/SARIF/JUnit) and dashboards; optional delivery to integrations (Slack, Jira, PagerDuty) and AI-assisted prioritisation/remediation on redacted findings. Purpose: providing the Customer with a Kubernetes security audit.

E. Duration

Raw artifacts: ≤ 24 hours (auto-deleted). Aggregate outputs and account data: for the term of the Service, then deleted or returned per §4.6.

Annex II — Technical & Organisational Measures

- **Encryption.** TLS in transit; encryption at rest for object storage and the control-plane database.
- **Data residency.** Region-pinned EU and US data planes; storage and control-plane DB do not cross regions (see §5).
- **Data minimisation & redaction.** Secrets and known sensitive fields are redacted at collection; AI prompts use redacted findings only (no secrets, no raw manifests).
- **Retention & verifiable deletion.** Raw artifacts auto-delete within 24 hours; deletions are recorded in an append-only, ed25519-signed retention log.
- **Access control.** Role-based access control (four roles; team-lead namespace scoping). Refresh tokens in HttpOnly cookies; short-lived (15-minute) in-memory access tokens.
- **Authentication.** JWT (HS256) access tokens; bcrypt-hashed passwords.
- **Offline scanning.** Scanners read collected manifests only and never connect to live customer clusters.
- **Ephemeral compute.** Cloud scan workers are ephemeral VMs that self-terminate after a job; a purge function acts as a safety net. Secrets are never baked into VM images.
- **Monitoring.** Error monitoring via an EU-hosted provider capturing stack traces and request metadata, excluding cluster data.
- **Egress control.** Outbound webhooks are constrained by an SSRF-protected IP-pinned allowlist of provider / customer-verified domains.

ANNEX III

Annex III — Authorised Sub-processors

Region indicates where the relevant Processing happens for EU tenants. Regions and contracts to be confirmed by legal/ops before publication.

Sub-processor	Purpose	Region	Data
Scaleway	Compute, object storage, control-plane DB, transactional email (EU)	**EU (FR)**	Cluster dumps, findings, PDFs, account data, email address, notification content
DigitalOcean	Compute + Spaces (US region)	**US**	US-tenant dumps, findings, PDFs
BunnyCDN (bunny.net)	Static asset CDN / edge	**EU-config**	Marketing site assets only
Mistral AI	LLM for EU tenants (direct, in-region)	**EU (FR)**	Redacted findings text only — see §5.2
Anthropic	LLM for US tenants (direct, in-region)	**US**	Redacted findings text only (US tenants) — see §5.2
Sentry	Error monitoring	**EU (DE)**	Stack traces, request metadata (no cluster data)
iubenda	Consent management / cookie banner	**EU**	Consent records
Plausible (Plausible Insights OÜ)	Privacy-friendly analytics	**EU**	Aggregate page views (no cookies, no PII)
Tawk.to	Live chat widget (marketing site)	**US**	Chat messages the visitor sends

END OF AGREEMENT · GENERATED FROM DOCS/LEGAL/DPA/DPA.HTML