Data Sitr Est. Privacy Policy

Generated: 2026-04-20T21:56:19Z

Source document: docs/privacy-policy.md

Git commit: 11283df

Generator: [operator-tooling]

Benchmark artifact: docs/generated/pii_benchmark_latest.json (generated 2026-04-20T03:31:24Z, Arabic NER loaded, 1K p95 31.48 ms)

Version: 1.0

Effective date: 2026-04-04

Applies to: DataSitr public site, dashboard, API, and operator-run deployments unless a signed customer agreement or deployment-specific notice states otherwise.

---

1. Entity name and activity

Data Sitr Est. operates **DataSitr**, a Saudi-hosted AI privacy gateway. DataSitr is designed to help enterprise customers process AI-bound text through a three-lane privacy model that detects personal data, tokenizes or routes it according to risk, and records machine-readable compliance metadata.

DataSitr is a technical control layer. It is not by itself a regulator approval, legal opinion, or standalone compliance determination.

---

2. Contact information and update record

Controller / operator contact

- Entity: Data Sitr Est.
- General privacy contact: `contact@datasitr.com`
- Security disclosure contact: `security@datasitr.com`
- Privacy and Compliance function: founder-led
- Interim Data Protection Officer (DPO): the founder of Data Sitr Est. currently serves this role
- DPO contact route: `dpo@datasitr.com`
- Direct public phone line: not separately published at this stage; requests are routed through the published contact address

Update record

Version	Date	Change

1.0	2026-04-04	First structured privacy policy published in English

3. Categories of personal data

Depending on how the service is used, DataSitr may collect, receive, or process:

- Account and onboarding data: tenant name, contact details, role assignments, API credentials, SSO metadata
- Submitted request data: text payloads sent through the API or dashboard
- Detected identifiers in those payloads: names, Saudi national IDs, Iqama, phone numbers, IBAN, email addresses, addresses, and similar direct identifiers
- Higher-risk or sensitive signals: health, biometric, genetic, criminal, ethnic-origin, religious, political, union-membership, sexual-orientation, credit, and location-tracking signals where detected
- Operational metadata: request IDs, timestamps, route decisions, provider selection, usage and billing records, webhook delivery status, and audit events
- Compliance records: processing records, transfer register events, subject-rights records, DPIA / RoPA outputs, and related evidence metadata

DataSitr is designed not to retain original request plaintext beyond the processing transaction unless an operator explicitly enables a feature that requires longer retention. Vaulted token mappings and compliance metadata may remain for the configured retention window.

4. Collection methods and purposes

Data Sitr Est. processes personal data through the following collection paths:

- **Direct collection from customers:** onboarding, API key creation, dashboard access, support requests, and configuration
- **Indirect collection through customer payloads:** personal data that appears inside text submitted for AI processing

Purposes of processing include:

- detecting personal data and sensitive signals
- tokenizing, pseudonymizing, or routing requests through the appropriate privacy lane
- supporting AI processing requested by the customer
- preserving auditability, processing records, transfer records, and subject-rights operations
- operating billing, support, incident response, and platform security workflows

The legal basis depends on the deployment and customer workflow. Typical bases include contract, legitimate interest, legal obligation, or consent where the customer chooses to rely on consent.

5. Processing mechanisms

DataSitr processes requests through a three-lane model:

- **Green lane:** detector-sanitized and tokenized text may be sent to approved external AI providers when the policy allows it
- **Amber lane:** pseudonymized text is intended to remain on operator-configured in-Kingdom processing paths
- **Red lane:** higher-risk or sensitive text is intended to remain on stricter in-Kingdom paths or be blocked
- **Block:** the request is rejected when policy or runtime controls do not allow a safe path

Detected identifiers are stored as encrypted vault mappings so they can be restored in the response when appropriate. DataSitr also writes machine-readable processing records, transfer events, and audit events.

---

6. Data sharing and disclosure

Data Sitr Est. may disclose or route data only as needed for service operation:

- to external AI providers for eligible green-lane requests, after tokenization and post-tokenization checks
- to operator-configured in-Kingdom providers for amber or red handling paths
- to infrastructure, support, or security subprocessors that the operator has configured for the deployment
- to legal or regulatory authorities where disclosure is required by law

DataSitr does not sell customer personal data and does not share it for advertising or unrelated marketing.

Cross-border disclosure is limited by the lane model, but Data Sitr Est. does not claim that technical routing alone replaces the need for customer-specific transfer assessments, contracts, or legal review.

---

7. Storage, retention, destruction, and security

Storage

- encrypted vault data and operational state are intended to remain on Saudi-hosted infrastructure in the standard deployment model
- compliance records are stored in append-only local logs or PostgreSQL shared-state, depending on deployment mode

Retention

- vaulted token mappings: deployment-configurable; current default target is short-lived retention
- processing and compliance records: up to 5 years where that retention schedule is configured for PDPL/SDAIA-aligned evidence keeping
- billing and usage records: retained according to operational, accounting, and contractual needs

Destruction

- expired vault entries are automatically removed by cleanup jobs
- subject-linked data can be deleted through supported subject-rights workflows
- deleted data is removed from active stores while required audit trails remain

Security measures

- AES-256-GCM encryption for vaulted values
- per-tenant key derivation
- role-based access control
- audit logging and integrity metadata
- HTTPS/TLS in transit
- guarded deployment and backup/restore procedures
- additional key-custody controls where configured for the deployment

---

8. Data subject rights

DataSitr supports workflows that help the customer or operator respond to:

- right of access
- right to rectification
- right to erasure
- complaint intake and audit logging

Where consent is the relied-on legal basis, withdrawal requests are handled through the privacy/compliance process defined by the operator and customer agreement.

Data subject requests should be sent to `support@datasitr.com` or through the customer's contracted support channel. The current operational target is to acknowledge requests promptly and complete supported workflows within **30 calendar days**, unless law or contract requires a different timeframe.

---

9. Complaints and objections

Data subjects or customers can:

- submit a complaint or objection to Data Sitr Est. through `contact@datasitr.com`
- report security issues to `security@datasitr.com`
- escalate to SDAIA or other competent authorities where applicable

The current internal target is to review complaint submissions within **5 business days** and issue a documented response or next-step notice within **30 calendar days**, unless a stricter legal or contractual timeline applies.

---

10. Policy access, language, and updates

This policy is published:

- on the public DataSitr site
- through the dashboard legal footer
- in the project documentation repository

Languages:

- English
- Arabic

Review schedule:

- at least annually
- after material changes to processing, routing, retention, subprocessors, or legal posture

For material changes, Data Sitr Est. may notify affected customers through the dashboard, email, or another agreed communication channel.

This document describes technical design intent and current operational posture. It does not constitute a warranty, service-level agreement, legal guarantee, or certification of regulatory compliance. DataSitr is designed to support PDPL alignment; it does not itself grant compliance. For the canonical list of safe and unsafe claims, contact gov@datasitr.com.